Ninth Edition

MICHAEL J. QUINN

ETHICS

FOR THE INFORMATION AGE

Ethics for the Information Age

9th edition

MICHAEL J. QUINN

Seattle University

221 River Street, Hoboken, NJ 07030

Content Management: Tracy Johnson
Content Production: Dr. Rajul Jain, Rajinder Singh
Product Management: Tracy Johnson
Product Marketing: Krista Clark
Rights and Permissions: Rogini Rajendiran, Chandan Kumar, Vignesh Murugamoorthy

Please contact www.AskPearsonSupport.com with any queries on this content.

Pearson puts care into the creation of our products. Our learning materials undergo content reviews to minimize bias and ensure the content is inclusive, accurate, and relevant. Please use this link to report instances of bias and inaccuracies: https://www.pearson.com/report-bias.html

You can learn more about Pearson's commitment to accessibility at https://www.pearson.com/us/accessibility.html

Cover Image by: Metamorworks/Shutterstock

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any

kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Copyright © 2025, 2020, 2017 by Pearson Education, Inc. or its affiliates, 221 River Street, Hoboken, NJ 07030. All Rights Reserved. Manufactured in the United States of America. This publication is protected by copyright, and permission should be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise. For information regarding permissions, request forms and the appropriate contacts within the Pearson Education Global Rights & Permissions department, please visit https://www.pearson.com/global-permission-granting.html.

Acknowledgments of third-party content appear on the appropriate page within the text.

PEARSON is exclusive trademark owned by Pearson Education, Inc. or its affiliates in the U.S. and/or other countries.

Unless otherwise indicated herein, any third-party trademarks that may appear in this work are the property of their respective owners and any references to third-party trademarks, logos or other trade dress are for demonstrative or descriptive purposes only. Such references are not intended

to imply any sponsorship, endorsement, authorization, or promotion of Pearson's products by the owners of such marks, or any relationship between the owner and Pearson Education, Inc. or its affiliates, authors, licensees or distributors.

Library of Congress Cataloging-in-Publication Data

Names: Quinn, Michael J. (Michael Jay), author.

Title: Ethics for the Information Age / Michael J. Quinn, Seattle University.

Description: Ninth edition. | Hoboken, NJ : Pearson, [2025] | Includes bibliographical references and index.

Identifiers: LCCN 2023057085 | ISBN 9780138238537 (hardcover)

Subjects: LCSH: Electronic data processing—Moral and ethical aspects. | Information technology—Moral and ethical aspects. | Computer networks—Moral and ethical aspects. | Computers and civilization.

Classification: LCC QA76.9.M65 Q56 2024 | DDC 004—dc23/eng/20240109

LC record available at https://lccn.loc.gov/2023057085

$PrintCode

ISBN-10: 0138238758

ISBN-13: 9780138238759

Brief Contents

Preface

1 Catalysts for Change

2 Introduction to Ethics

3 Networked Communications

4 Intellectual Property

5 Information Privacy

6 Privacy and the Government

7 Computer and Network Security

8 Computer Reliability

9 Professional Ethics

10 Automation and Globalization

Appendix A: Plagiarism

Appendix B: Introduction to Argumentation

Index

Contents

Preface

1 Catalysts for Change

1.1 Introduction

1.2 Milestones in Computing

1.2.1 Aids to Manual Calculating

1.2.2 Mechanical Calculators

1.2.3 Cash Register

1.2.4 Punched-Card Tabulation

1.2.5 Precursors of Commercial Computers

1.2.6 First Commercial Computers

1.2.7 Programming Languages and Time-Sharing

1.2.8 Transistor and Integrated Circuit

1.2.9 IBM System/360

1.2.10 Microprocessor

1.2.11 Personal Computer

1.3 Milestones in Networking

1.3.1 Electricity and Electromagnetism

1.3.2 Telegraph

1.3.3 Telephone

1.3.4 Typewriter and Teletype

1.3.5 Radio

1.3.6 Television

1.3.7 Remote Computing

1.3.8 ARPANET

1.3.9 Email

1.3.10 Internet

1.3.11 NSFNET

1.3.12 Broadband

1.3.13 Wireless Networks

1.3.14 Cloud Computing

1.4 Milestones in Information Storage and Retrieval

1.4.1 Greek Alphabet

1.4.2 Codex and Paper

1.4.3 Gutenberg's Printing Press

1.4.4 Newspapers

1.4.5 Hypertext

1.4.6 Graphical User Interface

1.4.7 Single-Computer Hypertext Systems

1.4.8 Networked Hypertext: World Wide Web

1.4.9 Search Engines

1.4.10 Cloud Storage

1.5 Contemporary Information Technology Issues

1.6 Views of Technology

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

2 Introduction to Ethics

2.1 Introduction

2.1.1 Defining Terms

2.1.2 Rationalizations

2.1.3 Four Scenarios

2.1.4 Overview of Ethical Theories

2.2 Subjective Relativism

2.2.1 The Case For Subjective Relativism

2.2.2 The Case Against Subjective Relativism

2.3 Cultural Relativism

2.3.1 The Case For Cultural Relativism

2.3.2 The Case Against Cultural Relativism

2.4 Divine Command Theory

2.4.1 The Case For the Divine Command Theory

2.4.2 The Case Against the Divine Command Theory

2.5 Ethical Egoism

2.5.1 The Case For Ethical Egoism

2.5.2 The Case Against Ethical Egoism

2.6 Kantianism

2.6.1 Good Will and the Categorical Imperative

2.6.2 Evaluating a Scenario Using Kantianism

2.6.3 The Case For Kantianism

2.6.4 The Case Against Kantianism

2.7 Act Utilitarianism

2.7.1 Principle of Utility

2.7.2 Evaluating a Scenario Using Act Utilitarianism

2.7.3 The Case For Act Utilitarianism

2.7.4 The Case Against Act Utilitarianism

2.8 Rule Utilitarianism

2.8.1 Basis of Rule Utilitarianism

2.8.2 Evaluating a Scenario Using Rule Utilitarianism

2.8.3 The Case For Rule Utilitarianism

2.8.4 The Case Against Utilitarianism in General

2.9 Social Contract Theory

2.9.1 The Social Contract

2.9.2 Rawls's Theory of Justice

2.9.3 Evaluating a Scenario Using Social Contract Theory

2.9.4 The Case For Social Contract Theory

2.9.5 The Case Against Social Contract Theory

2.10 Virtue Ethics

2.10.1 Virtues and Vices

2.10.2 Making a Decision Using Virtue Ethics

2.10.3 The Case For Virtue Ethics

2.10.4 The Case Against Virtue Ethics

2.11 Comparing Workable Ethical Theories

2.12 Morality of Breaking the Law

2.12.1 Social Contract Theory Perspective

2.12.2 Kantian Perspective

2.12.3 Rule-Utilitarian Perspective

2.12.4 Act-Utilitarian Perspective

2.12.5 Conclusion

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

3 Networked Communications

3.1 Introduction

3.2 Spam

3.2.1 The Spam Tsunami

3.2.2 Need for Social–Technical Solutions

3.2.3 Case Study: Anh the Acme Accountant

3.3 Internet Interactions

3.3.1 The World Wide Web

3.3.2 Mobile Apps

3.3.3 How We Use the Internet

3.4 Cryptocurrencies

3.4.1 Features of Cryptocurrencies

3.4.2 Uses of Cryptocurrencies

3.4.3 Sustainability Concerns

3.4.4 Financial Concerns

3.5 Text Messaging

3.5.1 Transforming Lives in Areas with Limited Infrastructure

3.5.2 Twitter

3.5.3 Business Promotion

3.6 Political Impact of Social Media and Online Advertising

3.6.1 Political Activism

3.6.2 Macedonian Entrepreneurs

3.6.3 Internet Research Agency

3.6.4 Is Democracy Being Threatened?

3.6.5 Troubling Times for Traditional Newspapers

3.7 Censorship

3.7.1 Direct Censorship

3.7.2 Self-Censorship

3.7.3 Challenges Posed by the Internet

3.7.4 Government Filtering and Surveillance of Internet Content

3.7.5 Ethical Perspectives on Censorship

3.8 Freedom of Expression

3.8.1 History

3.8.2 Freedom of Expression Not an Absolute Right

3.8.3 FCC v. Pacifica Foundation

3.8.4 Case Study: Leah's Blog

3.9 Children and Inappropriate Content

3.9.1 Web Filters

3.9.2 Child Internet Protection Act

3.9.3 Ethical Evaluations of CIPA

3.9.4 Sexting

3.10 Breaking Trust

3.10.1 Identity Theft

3.10.2 Fake Reviews

3.10.3 Online Predators

3.10.4 Ethical Evaluations of Police Sting Operations

3.10.5 False Information

3.10.6 Cyberbullying

3.10.7 Revenge Porn

3.11 Internet Addiction

3.11.1 Is Internet Addiction Real?

3.11.2 Contributing Factors to Addiction

3.11.3 Ethical Evaluation of Internet Addiction

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

4 Intellectual Property

4.1 Introduction

4.2 Intellectual Property Rights

4.2.1 Property Rights

4.2.2 Extending the Argument to Intellectual Property

4.2.3 Benefits of Intellectual Property Protection

4.2.4 Limits to Intellectual Property Protection

4.3 Protecting Intellectual Property

4.3.1 Trade Secrets

4.3.2 Trademarks and Service Marks

4.3.3 Patents

4.3.4 Copyrights

4.3.5 Non-fungible Tokens

4.3.6 Case Study: The Database Guru

4.4 Fair Use

4.4.1 *Sony v. Universal City Studios*

4.4.2 Audio Home Recording Act of 1992

4.4.3 *RIAA v. Diamond Multimedia*

4.4.4 *Kelly v. Arriba Soft*

4.4.5 *Authors Guild v. Google*

4.4.6 Mashups

4.5 Digital Media

4.5.1 Digital Rights Management

4.5.2 Digital Millennium Copyright Act

4.5.3 Secure Digital Music Initiative

4.5.4 Sony BMG Music Entertainment Rootkit

4.5.5 Criticisms of Digital Rights Management

4.5.6 Online Music Stores Drop Digital Rights Management

4.5.7 Microsoft Xbox One

4.6 Peer-to-Peer Networks and Cyberlockers

4.6.1 RIAA Lawsuits Against Napster, Grokster, and Kazaa

4.6.2 *MGM v. Grokster*

4.6.3 BitTorrent

4.6.4 Legal Action Against the Pirate Bay

4.6.5 PRO-IP Act

4.6.6 Megaupload Shutdown

4.6.7 Legal Online Access to Entertainment

4.7 Protections for Software

4.7.1 Software Copyrights

4.7.2 Violations of Software Copyrights

4.7.3 Safe Software Development

4.7.4 Software Patents

4.8 Legitimacy of Intellectual Property Protection for Software

4.8.1 Rights-Based Analysis

4.8.2 Utilitarian Analysis

4.8.3 Conclusion

4.9 Open-Source Software

4.9.1 Evolution of Proprietary Software

4.9.2 Consequences of Proprietary Software

4.9.3 “Open Source” Definition

4.9.4 Beneficial Consequences of Open-Source Software

4.9.5 Examples of Open-Source Software

4.9.6 The GNU Project and Linux

4.9.7 Impact of Open-Source Software

4.10 Creative Commons

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

5 Information Privacy

5.1 Introduction

5.2 Perspectives on Privacy

5.2.1 Defining Privacy

5.2.2 Harms and Benefits of Privacy

5.2.3 Is There a Natural Right to Privacy?

5.2.4 Privacy and Trust

5.2.5 Case Study: The New Parents

5.3 Information Disclosures

5.3.1 Public Records

5.3.2 Information Held by Private Organizations

5.3.3 Facebook Tags

5.3.4 Enhanced 911 Services

5.3.5 Rewards or Loyalty Programs

5.3.6 Body Scanners

5.3.7 RFID Tags

5.3.8 Implanted Chips

5.3.9 Mobile Apps

5.3.10 Facebook Login

5.3.11 OnStar

5.3.12 Automobile “Black Boxes”

5.3.13 Medical Records

5.3.14 Digital Video Recorders

5.3.15 Cookies

5.4 Data Mining

5.4.1 Data Mining Defined

5.4.2 Opt-In Versus Opt-Out Policies

5.4.3 Examples of Data Mining

5.4.4 Social Network Analysis

5.4.5 Release of "Anonymized" Datasets

5.5 Examples of Consumer or Political Backlash

5.5.1 Marketplace: Households

5.5.2 Facebook Beacon

5.5.3 Malls Track Shoppers' Cell Phones

5.5.4 iPhone Apps Uploading Address Books

5.5.5 Instagram's Proposed Change to Terms of Service

5.5.6 The *Daily Telegraph*

5.5.7 Cambridge Analytica

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

6 Privacy and the Government

6.1 Introduction

6.2 US Legislation Restricting Information Collection

6.2.1 Employee Polygraph Protection Act

6.2.2 Children's Online Privacy Protection Act

6.2.3 Genetic Information Nondiscrimination Act

6.3 Information Collection by the Government

6.3.1 Census Records

6.3.2 Internal Revenue Service Records

6.3.3 FBI National Crime Information Center 2000

6.3.4 National Data Exchange

6.3.5 Closed-Circuit Television Cameras

6.3.6 Police Misuse of Facial Recognition Systems

6.3.7 License-Plate Scanners

6.3.8 Police Drones

6.4 Covert Government Surveillance

6.4.1 Wiretaps and Bugs

6.4.2 Operation Shamrock

6.4.3 Carnivore Surveillance System

6.4.4 Covert Activities After 9/11

6.5 US Legislation Authorizing Wiretapping

6.5.1 Title III

6.5.2 Foreign Intelligence Surveillance Act

6.5.3 Electronic Communications Privacy Act

6.5.4 Stored Communications Act

6.5.5 Communications Assistance for Law Enforcement Act

6.6 USA PATRIOT Act

6.6.1 Provisions of the Patriot Act

6.6.2 National Security Letters

6.6.3 Responses to the Patriot Act

6.6.4 Successes and Failures

6.6.5 Long-Standing NSA Access to Telephone Records

6.7 Regulation of Public and Private Databases

6.7.1 Code of Fair Information Practices

6.7.2 Privacy Act of 1974

6.7.3 Fair Credit Reporting Act

6.7.4 Fair and Accurate Credit Transactions Act

6.7.5 Financial Services Modernization Act

6.8 Data Mining by the Government

6.8.1 Internal Revenue Service Audits

6.8.2 Syndromic Surveillance Systems

6.8.3 Telecommunications Records Database

6.8.4 Potential Harms of Profiling

6.9 National Identification Card

6.9.1 History and Role of the Social Security Number

6.9.2 Debate over a National ID Card

6.9.3 The REAL ID Act

6.10 Information Dissemination

6.10.1 Family Education Rights and Privacy Act

6.10.2 Video Privacy Protection Act

6.10.3 Health Insurance Portability and Accountability Act

6.10.4 Freedom of Information Act

6.10.5 Tollbooth Records Used in Court

6.10.6 *Carpenter v. United States*

6.11 Invasion

6.11.1 Telemarketing

6.11.2 Loud Television Commercials

6.11.3 Requiring Identification for Pseudoephedrine Purchases

6.11.4 Advanced Imaging Technology Scanners

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

7 Computer and Network Security

7.1 Introduction

7.2 Hacking

7.2.1 How Hackers Get Passwords

7.2.2 Penalties for Hacking

7.2.3 Selected Hacking Incidents

7.2.4 FBI and the Locked iPhone

7.2.5 Case Study: Firesheep

7.3 Malware

7.3.1 Viruses

7.3.2 The Internet Worm

7.3.3 Cross-Site Scripting

7.3.4 Drive-By Downloads

7.3.5 Trojan Horses and Backdoor Trojans

7.3.6 Ransomware

7.3.7 Rootkits

7.3.8 Spyware and Adware

7.3.9 Bots and Botnets

7.3.10 Security Risks Associated with “Bring Your Own Device”

7.4 Cyber Crime and Cyber Attacks

7.4.1 Phishing and Spear Phishing

7.4.2 SQL Injection

7.4.3 Denial-of-Service and Distributed Denial-of-Service Attacks

7.4.4 Internet-of-Things Devices Co-opted for DDoS Attack

7.4.5 Cyber Crime

7.4.6 Politically Motivated Cyber Attacks

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

8 Computer Reliability

8.1 Introduction

8.2 Data-Entry or Data-Retrieval Errors

8.2.1 Disenfranchised Voters

8.2.2 False Arrests

8.2.3 Utilitarian Analysis: Accuracy of NCIC Records

8.3 Software and Billing Errors

8.3.1 Errors Leading to System Malfunctions

8.3.2 Errors Leading to System Failures

8.3.3 Analysis: E-Retailer Posts Wrong Price, Refuses to Deliver

8.4 Notable Software System Failures

8.4.1 Patriot Missile

8.4.2 Ariane 5

8.4.3 AT&T Long-Distance Network

8.4.4 Robot Missions to Mars

8.4.5 Denver International airport

8.4.6 Tokyo Stock Exchange

8.4.7 Direct-Recording Electronic Voting Machines

8.5 Therac-25

8.5.1 Genesis of the Therac-25

8.5.2 Chronology of Accidents and AECL Responses

8.5.3 Software Errors

8.5.4 Postmortem

8.5.5 Moral Responsibility of the Therac-25 Team

8.5.6 Postscript

8.6 Tesla Version 7.0 (Autopilot)

8.6.1 Introduction

8.6.2 May 2016 Fatal Accident

8.6.3 The Hand-off Problem

8.6.4 Assigning Moral Responsibility

8.7 Uber Test-Vehicle Accident

8.7.1 Introduction

8.7.2 Shift to One Human Safety Operator

8.7.3 Effort to Eliminate “Bad Experiences”

8.7.4 March 18, 2018, Accident

8.8 Boeing 737 MAX

8.8.1 Background

8.8.2 Engineering Challenges and Solutions

8.8.3 Lack of Full Disclosure

8.8.4 Lion Air Flight 610

8.8.5 Consequences of the Lion Air Crash

8.8.6 Ethiopian Airlines Flight 302

8.8.7 Consequences of the Ethiopian Airlines Crash

8.8.8 Financial Impact of Crashes

8.8.9 Moral Responsibility of The Boeing Company

8.9 Algorithmic Bias

8.9.1 Bias in Computer Systems

8.9.2 Image Recognition Systems

8.9.3 Speech Recognition Systems

8.9.4 Impact Pro

8.9.5 Credit Scoring

8.9.6 Predictive Policing

8.9.7 COMPAS

8.9.8 Definitions of Fairness

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

9 Professional Ethics

9.1 Introduction

9.2 How Well Developed Are the Computing Professions?

9.2.1 Characteristics of a Fully Developed Profession

9.2.2 Case Study: Certified Public Accountants

9.2.3 How Do Computer-Related Careers Stack Up?

9.3 Software Engineering Code of Ethics

Preamble

Principles

9.4 Analysis of the Code

9.4.1 Preamble

9.4.2 Alternative List of Fundamental Principles

9.5 Case Studies

9.5.1 Software Recommendation

9.5.2 Child Pornography

9.5.3 Antiworm

9.5.4 Consulting Opportunity

9.6 Diversity, Equity, and Inclusion

9.6.1 Introduction

9.6.2 Gender Bias in Computing

9.6.3 Inclusive Language and Behavior

9.6.4 Best Practices

9.7 Whistle-Blowing

9.7.1 Morton Thiokol/NASA

9.7.2 Hughes Aircraft

9.7.3 US Legislation Related to Whistle-Blowing

9.7.4 Morality of Whistle-Blowing

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

10 Automation and Globalization

10.1 Introduction

10.2 Automation and Employment

10.2.1 Automation and Job Destruction

10.2.2 Automation and Job Creation

10.2.3 Time versus Possessions

10.2.4 Case Study: The Canceled Vacation

10.3 Breakthroughs in Artificial Intelligence

10.3.1 Introduction

10.3.2 ChatGPT

10.3.3 Deepfakes

10.3.4 Artificial General Intelligence

10.3.5 Ethics of Artificial Intelligence

10.3.6 Case Study: Autonomous Vehicles

10.4 Workplace Changes

10.4.1 Organizational Changes

10.4.2 Remote Work and Hybrid Work

10.4.3 The Gig Economy

10.4.4 Monitoring

10.4.5 Multinational Teams

10.5 Globalization

10.5.1 Arguments For Globalization

10.5.2 Arguments Against Globalization

10.5.3 Dot-Com Bust Increased IT Sector Unemployment

10.5.4 People from Other Countries Working in the US IT Industry

10.5.5 International Competition

10.5.6 Electronic Waste

10.6 The Digital Divide

10.6.1 Global Divide

10.6.2 Social Divide

10.6.3 Models of Technological Diffusion

10.6.4 Critiques of the Digital Divide

10.6.5 Online Courses

10.6.6 Net Neutrality

10.7 The "Winner-Take-All" Society

10.7.1 Harmful Effects of Winner-Take-All

10.7.2 Reducing Winner-Take-All Effects

Summary

Further Reading, Listening, and Viewing

Review Questions

Discussion Questions

In-Class Exercises

References

Appendix A: Plagiarism

Consequences of Plagiarism

Types of Plagiarism

Guidelines for Citing Sources

How to Avoid Plagiarism

Misuse of Sources

Additional Information

References

Appendix B: Introduction to Argumentation

B.1 Introduction

B.1.1 Arguments and Propositions

B.1.2 Conditional Statements

B.1.3 Backing

B.2 Valid Arguments

B.2.1 Affirming the Antecedent (Modus Ponens)

B.2.2 Denying the Consequent (Modus Tollens)

B.2.3 Process of Elimination

B.2.4 Chain Rule

B.3 Unsound Arguments

B.4 Common Fallacies

B.4.1 Affirming the Consequent

B.4.2 Denying the Antecedent

B.4.3 Begging the Question

B.4.4 Slippery Slope

B.4.5 Bandwagon Fallacy

B.4.6 Faulty Generalization (Hasty Generalization)

B.4.7 Division Fallacy

B.4.8 The Fallacy of Equivocation

B.5 Unfair Debating Gambits

B.5.1 Red Herring

B.5.2 Ad Hominem Argument

B.5.3 Attacking a Straw Man

B.6 Writing Persuasive Essays

The Government Should Ban Self-Driving Cars

Quiz

Answers to the Quiz Questions

References

Index

Preface

Computers and high-speed communication networks are transforming our world. These technologies have brought us many benefits, but they have also raised many social and ethical concerns. My view is that we ought to approach every new technology in a thoughtful manner, considering not just its short-term benefits, but also how its long-term use will affect our lives. A thoughtful response to information technology requires a basic understanding of its history, an awareness of current information-technology-related issues, and a familiarity with ethics. I have written *Ethics for the Information Age* with these ends in mind.

Ethics for the Information Age is suitable for college students at all levels. The only prerequisite is some experience using computers and the Internet. The book is appropriate for a stand-alone "computers and society" or "computer ethics" course offered by a computer science, business, or philosophy department. It can also be used as a supplemental textbook in a technical course that devotes some time to social and ethical issues related to computing.

As students discuss controversial issues related to information technology, they have the opportunity to learn from one other and improve their critical thinking skills. The provocative questions raised at the end of every chapter, together with dozens of in-class exercises, provide many opportunities for students to express their views, learn from their classmates, and refine their positions on important issues. My hope is that through these discussions students will get better at evaluating complex issues and defending their conclusions with facts, sound values, and rational arguments.

What's New in the Ninth Edition

The most significant change in the ninth edition is the addition of material that ensures coverage of every knowledge unit in the Society, Ethics and Professionalism knowledge area of the beta version of ACM/IEEE-CS/AAAI Computer Science Curricula 2023, including:

- issues related to improving diversity, equity, and inclusion

- algorithmic bias in facial recognition systems, speech recognition systems, healthcare management systems, credit scoring, recidivism prediction, and predictive policing
- economies of computing, such as monopolies, open versus closed platforms, pricing strategies, and cryptocurrencies
- issues related to sustainability, such as resource consumption of information technology, proof-of-work versus proof-of-stake algorithms, feedback systems to promote sustainable behavior, and e-waste
- philosophical views of technology, including instrumentalism, neutrality thesis, pragmatism, technological determinism, cultural approaches to technology, and decolonial technical design

The ninth edition also covers many more new developments and controversies related to the introduction, use, and abuse of information technology in modern society, including:

- breakthroughs in artificial intelligence, including generative AI (particularly ChatGPT) and AI ethics
- detailed examination of the fatal crashes of the Boeing 737 MAX

- impact of the COVID-19 pandemic on remote work
- discussion of ethical rationalizations (also called moral excuses)
- non-fungible tokens as intellectual property
- role of social media in George Floyd protests
- role of social media in January 6, 2021 assault on US Capitol
- ransomware attacks on Colonial Pipeline
- Russia's cyberattacks on Ukraine
- privacy concerns related to machine learning

Finally, I have updated a significant number of facts and figures throughout the book.

Organization of the Book

The book is divided into 10 chapters. Chapter 1 has several objectives: to get the reader thinking about how social conditions can lead to the development of new technologies and how the adoption of new technologies can lead to social change; to provide the reader with an introduction to the history of computing, networking, and information storage

and retrieval; and to help the reader understand how the introduction of information technology has raised some new ethical issues.

Chapter 2 is an introduction to ethics. It presents nine different theories of ethical decision making, weighing the pros and cons of each one. Five of these theories—Kantianism, act utilitarianism, rule utilitarianism, social contract theory, and virtue ethics—are deemed the most appropriate "tools" for analyzing moral problems in the remaining chapters.

Chapters 3–10 discuss a wide variety of issues related to the introduction of information technology into society. I think of these chapters as forming concentric rings around a particular computer user.

Chapter 3 is the innermost ring, focusing on communications over cellular networks and the Internet. Issues such as the increase in spam, political activism over social media, government censorship, identity theft, sexting, revenge porn, and Internet addiction raise important questions related to trust, quality of life, free speech, and whether new media are strengthening or weakening democracies.

The next ring, Chapter 4, deals with the creation and exchange of intellectual property. It discusses intellectual property rights; legal safeguards for intellectual property; the definition of fair use; the impact of digital media, peer-to-peer networks, and cyberlockers; software copyrights and software patents; the legitimacy of intellectual property protection for software; and the rise of the open-source movement.

Chapter 5 focuses on information privacy. What is privacy exactly? Is there a natural right to privacy? How do others learn so much about us? The chapter examines the electronic trail that people leave behind when they use a cell phone, drive a car, search the Web, use social media, make credit card purchases, open a bank account, go to a physician, or apply for a loan, and it explains how mining data to predict consumer behavior has become an important industry. It also provides several examples where companies have gone too far with their collection of personal information, and the consumer or political backlash that has resulted.

Chapter 6 focuses on privacy and the US government. Using Daniel Solove's taxonomy of privacy as our organizing principle, I look at how the government has steered between the competing interests of personal privacy and public safety.

I consider US legislation to restrict information collection and government surveillance; government regulation of private databases and abuses of large government databases; legislation to reduce the dissemination of information and legislation that has had the opposite effect; and finally government actions to prevent the invasion of privacy as well as invasive government actions. Along the way, I discuss the implications of the USA PATRIOT Act and the debate over the REAL ID Act to establish a de facto national identification card in the United States.

Chapter 7 focuses on the vulnerabilities of networked computers. A case study focuses on the release of the Firesheep extension to the Firefox Web browser. A section on malware discusses viruses, worms, cross-site scripting, drive-by downloads, Trojan horses, ransomware, rootkits, spyware, botnets, and more. The chapter covers phishing, spear phishing, SQL injection, denial-of-service attacks, and distributed denial-of-service attacks, and how these tools are employed by criminal organizations and nation states.

Computerized system failures have led to inconvenienced consumers, lost income for businesses, the destruction of property, human suffering, and even death. Chapter 8 describes some notable software system failures, including the

story of the Therac-25 radiation therapy system. It also covers an important contemporary problem: the safety of self-driving automobiles. A new section focuses on the engineering and management decisions leading up to two fatal crashes of the Boeing 737 MAX. Another new section defines algorithmic bias, gives seven examples of deployed computer systems that have exhibited algorithmic bias, and discusses challenges facing designers who seek to create systems that exhibit fairness.

Chapter 9 is particularly relevant for those readers who plan to take jobs in the computer industry. The chapter presents a professional code related to computing, the Software Engineering Code of Ethics and Professional Practice, followed by an analysis of the code. Several case studies illustrate how to use the code to evaluate moral problems related to the use of computers. A new section focuses on diversity, equity, and inclusion: why it is an important topic, evidence of gender bias in computing, inclusive language and behavior, and best practices. The chapter concludes with an ethical evaluation of whistle-blowing, an extreme example of organizational dissent.

Chapter 10 raises a wide variety of issues related to how information technology has impacted the world of work and

the distribution of wealth. Topics include automation, the rise of computerized systems relying on artificial intelligence, remote work, workplace monitoring, the gig economy, and globalization. Does automation increase unemployment? Will improvements in artificial intelligence lead to most jobs being taken over by machines? Is there a "digital divide" separating society into "haves" and "have-nots"? Is information technology widening the gap between rich and poor? These are just a few of the important questions the chapter addresses. A new section focuses on the stunning breakthroughs in artificial intelligence, the capabilities and limitations of ChatGPT, the rise of deepfakes, perspectives on artificial general intelligence, efforts to develop guidelines for AI ethics, and a case study on autonomous vehicles.

Note to Instructors

In March 2023, a joint task force of the Association for Computing Machinery, the IEEE-Computer Society, and the Association for Advancement of Artificial Intelligence released a beta version of *Computer Science Curricula 2023* (csed.acm.org/). The report recommends that every undergraduate computer science degree program incorporate instruction related to Society, Ethics and Professionalism through "a combination of one required course along with

aspects integrated into other technical courses" (*Computer Science Curricula 2023, Version Beta*, p. 274). *Ethics for the Information Age* covers nearly all of the CS Core and KA Core topics described in the report, with the notable exception of Professional Communication. Table 1 shows the mapping between the other knowledge units within Society, Ethics and Professionalism and the chapters of this book.

Table 1

Name	Chapter(s) or Appendix
Social Context	3, 8, 10
Methods for Ethical Analysis	1, 2, 9, 10, B
Professional Ethics	8, 9
Intellectual Property	4, A
Privacy and Civil Liberties	3, 5, 6
Sustainability	3, 8, 10
History	1, 10
Economies of Computing	1, 3, 4, 10
Security Policies, Laws, and Computer Crimes	7
Equity, Diversity and Inclusion	1, 8, 9, 10

Mapping between the knowledge units of Society, Ethics and Professionalism in *Computer Science Curricula 2023* and the chapters of this book.

The organization of the book makes it easy to adapt to your particular needs. If your syllabus does not include the history of information technology, you can skip the middle three sections of Chapter 1 and still expose your students to examples motivating the formal study of ethics in Chapter 2. After Chapter 2, you may cover the remaining chapters in any order you choose, because Chapters 3–10 do not depend on one other.

Many departments choose to incorporate discussions of social and ethical issues throughout the undergraduate curriculum. The independence of Chapters 3–10 makes it convenient to use *Ethics for the Information Age* as a supplementary textbook. You can simply assign readings from the chapters most closely related to the course topic.

Supplements

The following supplements are available to qualified instructors on Pearson's Instructor Resource Center. Please contact your local Pearson sales representative or visit www.pearsonhighered.com/educator to access this material.

- An instructor's manual provides tips for teaching a course in computer ethics. It also contains answers to all of the review questions.
- A test bank contains more than 500 multiple-choice, fill-in-the-blank, and essay questions that you can use for quizzes, midterms, and final examinations.
- A set of PowerPoint lecture slides outlines the material covered in every chapter.

Feedback

Ethics for the Information Age cites over a thousand sources and includes dozens of ethical analyses. Despite my best efforts and those of many reviewers, the book is bound to contain errors. I appreciate getting comments (both positive and negative), corrections, and suggestions from readers. You can reach me through my Web site: www.michaeljquinn.net.

Acknowledgments

I appreciate the support provided by a fine publications team at Pearson Education, starting with Tracy Johnson, higher education global content manager, and including associate content producer Rajul Jain, senior producer Pallavi Pandit,

director of production Ashley Santora, assistant managing producer Rajinder Singh, and associate analyst Erin Sullivan.

A superb group of reviewers provided me with many helpful suggestions regarding new material to incorporate into the ninth edition. Four of them agreed to be recognized publicly. My thanks to Amy Bruckman, Georgia Tech; Dianne Hansford, Arizona State University; Richard LeBlanc, Seattle University; and Kanika Sood, California State University, Fullerton.

I want to recognize all who participated in the creation of the first eight editions or provided useful suggestions for the ninth edition: Paul Anagnostopoulos, Valerie Anctil, Beth Anderson, Bob Baddeley, George Beekman, Brian Breck, Maria Carl, Sherry Clark, Nathan Colaner, Thomas Dietterich, Roger Eastman, Beverly Fusfield, Robert Greene, Jose Guerrero, Peter Harris, Susan Hartman, Michael Hirsch, Michael Johnson, Paulette Kidder, Marilyn Lloyd, Pat McCutcheon, Joshua Noyce, Beth Paquin, Konrad Puczynski, Brandon Quinn, Courtney Quinn, Stuart Quinn, Victoria Quinn, Matthew Rellihan, Charley Renn, Gregory Silverman, Lindsey Triebel, Charles Volzka, Shauna Weaver, and Todd Will.

Reviewers of previous editions include Ramprasad Bala, University of Massachusetts at Dartmouth; Phillip Barry, University of Minnesota; Bo Brinkman, Miami University; Diane Cassidy, University of North Carolina at Charlotte; Madhavi M. Chakrabarty, New Jersey Institute of Technology; John Clark, University of Colorado at Denver; Timothy Colburn, University of Minnesota Duluth; Lorrie Faith Cranor, Carnegie Mellon University; Lee D. Cornell, Minnesota State University, Mankato; Donna Maria D'Ambrosio, University of South Florida; Dawit Demissie, The Sage Colleges; J.C. Diaz, University of Tulsa; Richard W. Egan, New Jersey Institute of Technology; Rhonda Ficek, Minnesota State University Moorhead; Tom Gallagher, University of Montana; Fred Geldon, George Mason University; David Goodall, State University of New York at Albany; Richard E. Gordon, University of Delaware; Mike Gourley, University of Central Oklahoma; D.C. Grant, Columbia Basin College; Robert Greene, University of Wisconsin-Eau Claire; Fritz H. Grupe, University of Nevada, Reno; Ric Heishman, George Mason University; Micha Hofri, Worcester Polytechnic Institute; Gurdeep Hura, University of Maryland Eastern Shore; Musconda Kapatamoyo, Southern Illinois University, Edwardsville; Christopher Kauggman, George Mason University; Evelyn

Lulis, DePaul University; Tamara A. Maddox, George Mason University; Aparna Mahadev, Worcester State University; Eric Manley, Drake University; Richard D. Manning, Nova Southeastern University; James Markulic, New Jersey Institute of Technology; John G. Messerly, University of Texas at Austin; Linda O'Hara, Oregon State University; Joe Oldham, Centre College; Mimi Opkins, California State University, Long Beach; Daniel Palmer, Kent State University; Holly Patterson-McNeill, Lewis-Clark State College; Colin Potts, Georgia Tech; Jason Rogers, George Mason University; Medha S. Sarkar, Middle Tennessee State University; Michael Scanlan, Oregon State University; Robert Sloan, University of Illinois at Chicago; Matthew Stockton, Portland Community College; Dorothy Sunio, Leeward Community College; Leon Tabak, Cornell College; Renée Turban, Arizona State University; Scott Vitz, Indiana University–Purdue University Fort Wayne; Todd Will, New Jersey Institute of Technology; David Womack, University of Texas at San Antonio; John Wright, Juniata College; and Matthew Zullo, Wake Technical Community College.

Finally, I am indebted to my wife, Victoria, for her support and encouragement. You are a wonderful blessing to me, day in and day out! Thanks for everything.

Michael J. Quinn

Cedar Mill, Oregon

We never know how high we are
Till we are called to rise;
And then, if we are true to plan,
Our statures touch the skies.
The heroism we recite
Would be a daily thing,
Did not ourselves the cubits warp
For fear to be a king.

—Emily Dickinson, *Aspiration*

I dedicate this book to *Shauna*, *Skyler*, *Brandon*, *Courtney*, *Bridget*, and *Claire*.
Know that my love goes with you, wherever your aspirations may lead you.

Chapter 1

Catalysts for Change

1.1 Introduction

WE ARE LIVING IN THE INFORMATION AGE. NEVER BEFORE HAVE SO many people had such easy access to information. The two principal catalysts for the Information Age have been low-cost computers and high-speed communication networks, which have made possible the development of exciting new technologies, including smartphones, video streaming services, voice-activated digital assistants, low-cost drones, and self-driving cars (Figure 1.1).

Figure 1.1

Low- cost computers and high-speed communication networks make possible the products of the Information Age, such as the Samsung Galaxy S23 Ultra. It functions as a phone, text messager, email client, Web browser, camera, video recorder, digital compass, and much more.

(Framesira/Shutterstock)

Modern computing and communications systems have profoundly changed the way we live. In 1950 there were no more than a handful of electronic digital computers in the world, and the Internet did not exist. Today we are surrounded by networked devices containing embedded microprocessors, and most of us spend many hours every day engaged with them as we communicate, seek information, play games, listen to music, or watch videos.

The importance of modern information technology was dramatically illustrated during the COVID-19 pandemic. Billions of people around the world suddenly found themselves in lockdown, totally dependent on their digital devices, not just for news and entertainment, but to do their jobs or attend school as well [**1**]. The pandemic also highlighted the "digital divide." Students living in homes with up-to-date computers and high-speed Internet access were able to engage in online learning, but millions of students from low-income families could not participate fully and fell behind in their studies [**2**].

Our relationship with technology is complicated. We create technology and choose to adopt it. However, once we have adopted a technological device, it can transform us and how we relate to other people and our environment.

Some of the transformations are physical. The neural pathways and synapses in our brains demonstrate neuroplasticity: literally changing with our experiences. The US Surgeon General has warned that frequent use of social media by adolescents can affect the development of their brains' amygdala and prefrontal cortex, increase their "sensitivity to social rewards and punishments," and decrease life satisfaction, particularly for girls aged 11–13 and boys aged 14–15 [**3**].

Studies with macaque monkeys suggest that when we satisfy our hunger for quick access to information through our use of Web browsers, Facebook, Twitter, and texting, neurons inside our brains release dopamine, producing a desire to seek out additional information, causing further releases of dopamine, and so on, which may explain why we find it difficult to break away from these activities [**4**, **5**].

Adopting a technology can change our perceptions, too. More than 90 percent of cell phone users report that having a cell phone makes them feel safer, but once people get used to carrying a cell phone, losing the phone may make them feel more vulnerable than they ever did before they began carrying one. A Rutgers University professor asked his students to go without their cell phones for 48 hours. Some

students couldn't do it. A student reported to the student newspaper, "I felt like I was going to get raped if I didn't have my cell phone in my hand." Some caregivers purchase cell phones for children so that a child may call a family member in an emergency. However, caregivers who provide a cell-phone "lifeline" may be implicitly communicating to the children the idea that people in trouble cannot expect help from strangers [**6**].

The Amish understand that the adoption of a new technology can affect the way people relate to each other (Figure 1.2). Amish bishops meet twice a year to discuss matters of importance to the church, including whether any new technologies should be allowed. Their discussion about a new technology is driven by the question, "Does it bring us together, or draw us apart?" You can visit an "Old Order" Amish home and find a gas barbecue on the front porch but no telephone inside, because they believe gas barbecues bring people together while telephones interfere with face-to-face conversations [7].

Figure 1.2

Most of us appreciate the many beneficial changes that technology has brought into our lives. In health care alone, computed tomography (CT) and magnetic resonance imaging (MRI) scanners have greatly improved our ability to diagnose major illnesses; new vaccines and pharmaceuticals have eradicated some deadly diseases and brought others under control; and pacemakers, hearing aids, and artificial joints have improved the physical well-being of millions.

New technologies are adopted to solve problems, but they often create problems, too. The automobile has given people the ability to travel where they want, when they want. On the other hand, millions of people spend an hour or more each day stuck in traffic commuting between home and work. Commuters frustrated by slow freeway traffic turn to mobile apps like Waze to find shortcuts, but when too many drivers follow these apps, long lines at exit ramps can actually

increase freeway congestion for the remaining vehicles, and cars taking shortcuts can overwhelm side streets and clog intersections, frustrating local residents [8]. The Web contains billions of pages and makes possible extraordinarily valuable information retrieval systems. Even grade-school children are expected to gather information from the Web when writing their reports. However, many caregivers worry that their Web-surfing children may be exposed to pornographic or violent images or other inappropriate material. New communication technologies have made it possible for us to get access to news and entertainment from around the world. However, the same technologies have enabled major software companies to move thousands of jobs to India, China, and Vietnam. The people and economies of India, China, and Vietnam benefit from the new software jobs, but computer programmers in the United States experience a downward pressure on their salaries [9].

We may not be able to prevent a new technology from being invented, but we do have control over whether to adopt it. Nuclear power is a case in point. Nuclear power plants create electricity without producing carbon dioxide emissions, but they also produce radioactive waste products that must be safely stored for 100,000 years. Although nuclear power technology was available, 67 nuclear reactor construction

projects were canceled after the accident at Three Mile Island in 1979 [**10**].

Finally, we *can* influence the rate at which new technologies are developed. Some societies, such as the United States, have a history of nurturing and exploiting new inventions. Congress has passed intellectual property laws that allow people to make money from their creative work, and the federal income tax structure allows individuals who create popular new technologies to accumulate great wealth.

To sum up, societies develop new technologies to solve problems or make life better, but the use of new technologies changes social conditions and may create new problems. That doesn't mean we should never adopt a new technology, but it does give us a good reason why we should be making informed decisions, weighing the benefits and potential harms associated with the use of new devices. To that end, this book will help you gain a better understanding of contemporary ethical issues related to the use of information technology.

This chapter sets the stage for the remainder of the book. Electronic digital computers and high-performance communication networks are central to contemporary information technology. While the impact of these inventions

has been dramatic in the past few decades, their roots go back hundreds of years. Section 1.2 tells the story of the development of computers, showing how they evolved from simple manual calculation aids to complex microprocessors. In Section 1.3 we describe two centuries of progress in networking technology, starting with the semaphore telegraph and culminating in the creation of an email system connecting over a billion users. Section 1.4 shows how information storage and retrieval evolved from the creation of the Greek alphabet to Google. Section 1.5 discusses some of the moral issues that have arisen from the deployment of information technology. Finally, Section 1.6 illustrates how the way people approach these contemporary moral issues depends on their philosophical views of the role of technology in society.

1.2 Milestones in Computing

Calculating devices have supported the development of commercial enterprises, governments, science, and weapons. As you will see in this section, the introduction of new technologies has often had a social impact.

1.2.1 Aids to Manual Calculating

Adding and subtracting are as old as commerce and taxes. Fingers and toes are handy calculation aids, but to manipulate larger numbers, people need more than their own digits. The tablet, the abacus, and mathematical tables are three important aids to manual calculating [**11**].

Simply having a tablet to write down the numbers being manipulated is a great help. In ancient times, erasable clay and wax tablets served this purpose. By the late Middle Ages, Europeans often used erasable slates. Paper tablets became

common in the nineteenth century, and they are still popular today.

An **abacus** is a computing aid in which a person performs arithmetic operations by sliding counters along rods, wires, or lines. The first abacus was probably developed in the Middle East more than 2,000 years ago. In a Chinese, Japanese, or Russian abacus, counters move along rods or wires held in a rectangular frame. Beginning in medieval Europe, merchants performed their calculations by sliding wooden or metal counters along lines drawn on a wooden counting board (Figure 1.3). Eventually, the word "counter" came to mean not only the disk being manipulated but also the place in a store where transactions take place [**11**].

Figure 1.3

Mathematical tables have been another important aid to manual computing for about 2,000 years. A great breakthrough occurred in the early seventeenth century, when John Napier and Johannes Kepler published tables of logarithms. These tables were tremendous time-savers to anyone doing complicated math because they allowed them to multiply two numbers by simply adding their logarithms. Many other useful tables were created as well. For example, businesspeople consulted tables to compute interest and convert between currencies. Today people who compute their income taxes “by hand” use tax tables to determine how much they owe.

Even with tablets, abacuses, and mathematical tables, manual calculating is slow, tedious, and error-prone. To make matters worse, mathematical tables prepared centuries ago usually contained errors. That’s because somebody had to compute each table entry and somebody had to typeset each entry, and errors could occur in either of these steps. Advances in science, engineering, and business in the post-

Renaissance period motivated European inventors to create new devices to make calculations faster and more reliable and to automate the printing of mathematical tables.

1.2.2 Mechanical Calculators

Blaise Pascal had a weak physique but a powerful mind. When he got tired of summing by hand long columns of numbers given him by his father, a French tax collector, he constructed a mechanical calculator to speed the chore. Pascal's calculator, built in 1640, was capable of adding whole numbers containing up to six digits. Inspired by Pascal's invention, the German Gottfried Leibniz constructed a more sophisticated calculator that could add, subtract, multiply, and divide whole numbers. The handcranked machine, which he called the Step Reckoner, performed multiplications and divisions through repeated additions and subtractions, respectively. The calculators of Pascal and Leibniz were not reliable, however, and did not enjoy commercial success.

In the nineteenth century, advances in machine tools and mass-production methods, combined with larger markets, made possible the creation of practical calculating machines.

Frenchman Charles Thomas de Colmar utilized the stepped-drum gear mechanism invented by Leibniz to create the Arithmometer, the first commercially successful calculator. Many insurance companies purchased Arithmometers to help their actuaries compute rate tables more rapidly [**11**].

English polymath Charles Babbage was intimately familiar with the manual production of mathematical tables. He resolved to build a machine capable of automatically calculating and typesetting table values. In 1822, Babbage began work on a difference engine to compute polynomial functions through the method of finite differences. Despite receiving substantial funding from the British government, Babbage never completed work on the difference engine. After the failure of the difference engine project, Babbage created designs for an Analytical Engine capable of general-purpose computation, though this machine, too, was never constructed.

Swedish publisher Georg Scheutz and his son Edvard developed their own designs for a difference engine and completed the world's first printing calculator: a machine capable of calculating mathematical tables and typesetting the values onto molds. The Dudley Observatory in Albany, New York, purchased the Scheutz difference engine in 1856.

With support from the US Nautical Almanac Office, astronomers used the machine to help them compute the motion of Mars and the refraction of starlight. Difference engines were never widely used; the technology was eclipsed by the emergence of simpler and less-expensive calculating machines [**11**].

The United States in the late 1800s was fertile ground for the development of new calculating technologies. This period of US history, commonly known as the Gilded Age, was characterized by rapid industrialization, economic expansion, and a concentration of corporate power. Corporations merged to increase efficiency and profits, but the new, larger corporate organizations had multiple layers of management and multiple locations. In order for middle- and upper-level managers to monitor and improve performance, they needed access to up-to-date, comprehensive, reliable, and affordable information. All these requirements could not be met by bookkeepers and accountants using pen and paper to sum long columns of transactions by hand [**12**].

To meet this demand, many entrepreneurs began producing adding and calculating machines. One of these inventors was William Burroughs, a former bank clerk who had spent long days adding columns of figures. Burroughs devised a practical

adding machine and offered it for sale. He found himself in a cutthroat market; companies competed fiercely to reduce the size of their machines and make them faster and easier to use. Burroughs distinguished himself from his competitors by putting together first-class manufacturing and marketing organizations, and by the 1890s the Burroughs Adding Machine Company led the industry. Calculating machines were entrenched in the offices of large US corporations by the turn of the century [**12**].

The adoption of mechanical calculators led to the "de-skilling" and "feminization" of bookkeeping (Figure 1.4). Before the introduction of calculating machines, offices were a bastion of men, and men who could rapidly compute sums by hand were at a premium. Calculators leveled the playing field, making people of average ability quite productive. In fact, a 1909 Burroughs study concluded that a clerk using a calculator was six times faster than a clerk adding the same column of figures by hand [**13**]. As managers introduced mechanical calculators into offices, they replaced men who were bookkeepers with women and lowered wages. In 1880 only 5.7 percent of bookkeepers, cashiers, and accountants were women, but by 1910 the number of women in these jobs had risen to 38.5 percent [**14**].

Figure 1.4

Mechanical calculators led to the “de-skilling” and “feminization” of bookkeeping.

(Science & Society Picture Library/SSPL/Getty Images)

1.2.3 Cash Register

Store owners in the late 1800s faced challenges related to accounting and embezzlement. Keeping accurate sales records was becoming more difficult as smaller stores evolved into “department stores” with several departments and many clerks. Preventing embezzlement was tricky when clerks could steal cash simply by not creating receipts for some sales.

While on a European holiday in 1878, Ohio restaurateur James Ritty saw a mechanical counter connected to the propeller shaft of his ship. A year later he and his brother John used that concept to construct the first cash register,

essentially an adding machine capable of expressing values in dollars and cents. Enhancements followed rapidly, and by the early 1900s the cash register had become an important information-processing device. Cash registers created printed, itemized receipts for customers, maintained printed logs of transactions, and performed other accounting functions that provided store owners with the detailed sales records they needed.

Cash registers also made embezzlement by clerks more difficult. The bell made it impossible for clerks to sneak money from the cash drawer and helped ensure that every sale was "rung up." Printed logs made it easy for department store owners to compare cash on hand against sales receipts [12].

1.2.4 Punched-Card Tabulation

As corporations and governmental organizations grew larger in the late 1800s, they needed to handle greater volumes of information. One of these agencies was the US Bureau of the Census, which collected and analyzed information on tens of millions of residents every decade. Aware of the tedium and errors associated with clerks manually copying and tallying

figures, several Census Bureau employees developed mechanical tabulating machines. Herman Hollerith created the most successful device. Unlike a predecessor, who chose to record information on rolls of paper, Hollerith decided to record information on punched cards. The use of punched cards to store data was a much better approach because cards could be sorted into groups, allowing the computation of subtotals by categories. Hollerith's equipment proved to be a great success when used in the 1890 census. In contrast to the 1880 census, which had required eight years to complete, the 1890 census was finished in only two years. Automating the census saved the Census Bureau five million dollars, about one-third of its annual budget [**15**].

Other data-intensive organizations found applications for punched cards. Railroads used them to improve their accounting operations and send bills out more frequently. Retail organizations, such as Marshall Field's, used punched cards to perform more sophisticated analyses of information generated by the cash registers at its many department stores. The Pennsylvania Steel Company and other heavy industries began to use punched-card technology to do cost accounting on manufacturing processes.

The invention of sorters, tabulators, and other devices to manipulate the data on punched cards created a positive feedback loop. As organizations began using tabulating machines, they thought up new uses for information-processing equipment, stimulating further technological innovations.

International Business Machines (IBM) is the corporate descendant of Hollerith's company. Over a period of several decades, IBM and its principal competitor, Remington Rand, developed sophisticated machines based on punched cards: card punches, card verifiers, card tabulators, card sorters, and alphabetizers. Customers used these devices to create **data-processing systems** that received input data, performed one or more calculations, and produced output data. Within these systems, punched cards stored input data, intermediate results, and output data. In the most complicated systems, punched cards also stored the program—the steps of the computational process to be followed. Early systems relied on human operators to carry cards from one machine to the next. Later systems had electrical connections that allowed the output of one machine to be transmitted to the next machine without the use of punched cards or human intervention.

Organizations with large data-processing needs found punched-card tabulators and calculators to be valuable devices, and they continually clamored for new features that would improve the computational capabilities and speed of their systems [**12**]. These organizations would become a natural market for commercial electronic digital computers.

Some customers of data-processing equipment used these systems for nefarious purposes. For example, IBM machines played an infamous role in the Holocaust. After Adolf Hitler came to power in Germany in 1933, IBM chief executive Thomas J. Watson overlooked well-publicized accounts of antisemitic violence and the opening of concentration camps, focusing instead on a golden business opportunity. The firm expanded the operations of its German subsidiary, Dehomag, built a new factory in Germany, and actively sought business from the German government. Tabulating, sorting, collating, and alphabetizing machines and support services provided by Dehomag allowed the Nazi government to conduct rapid censuses, identify acknowledged Jewish people and those with Jewish ancestors, and generate the alphabetical lists of names needed to efficiently seize their assets, confine them to ghettos, and deport them to death camps [**15**].

1.2.5 Precursors of Commercial Computers

Several computing devices developed during and immediately after World War II paved the way for the commercialization of electronic digital computers.

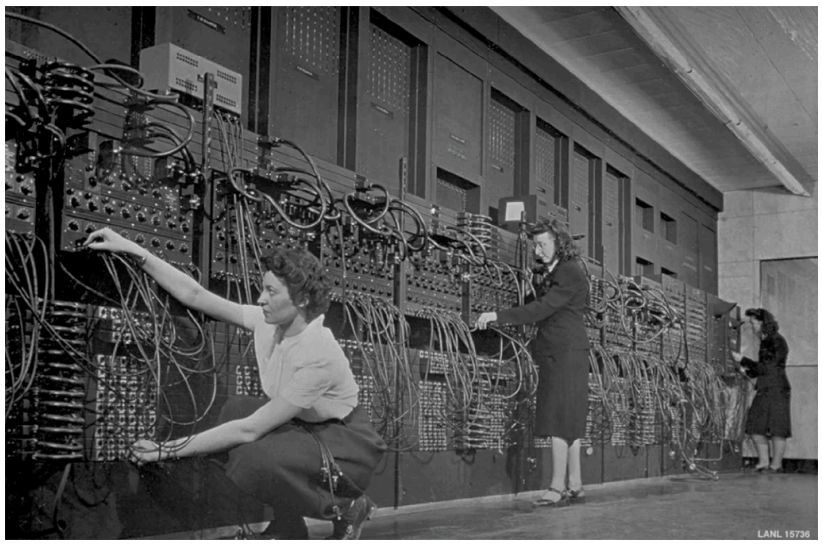
Between 1939 and 1941, Iowa State College professor John Atanasoff and his graduate student Clifford Berry constructed an electronic device for solving systems of linear equations. The Atanasoff-Berry Computer was the first computing device built with vacuum tubes, but it was not programmable.

Dr. John W. Mauchly, a physics professor at the University of Pennsylvania, visited Iowa State College in 1941 to learn more about the Atanasoff-Berry Computer. After he returned to Penn, Mauchly worked with J. Presper Eckert to create a design for an electronic computer to speed the computation of artillery tables for the US Army. They led a team that completed work on the ENIAC (electronic numerical integrator and computer) in 1946. As it turns out, the war ended before the ENIAC could provide the Army with any ballistics tables, but its speed was truly impressive. A person

with a desk calculator could compute a 60-second trajectory in 20 hours. The ENIAC performed the computation in 30 seconds. In other words, the ENIAC was 2,400 times faster than a person with a desk calculator.

The ENIAC had many features of a modern computer. All its internal components were electronic, and it could be programmed to perform a variety of computations. However, its program was not stored inside memory. Instead, it was "wired in" from the outside. Reprogramming the computer meant removing and reattaching many wires. This process could take many days (Figure 1.5).

Figure 1.5



The ENIAC's first six programmers were women. Every instruction was programmed by connecting several wires into plugboards.

(Historical/Corbis Historical/Getty Images)

Even before the ENIAC was completed, work began on a follow-on system called the EDVAC (electronic discrete variable automatic computer). The design of the EDVAC incorporated many improvements over the ENIAC. The most important improvement was that the EDVAC stored the program in primary memory, along with the data manipulated by the program. In 1946 Eckert, Mauchly, and several other computer pioneers gave a series of 48 lectures at the Moore School. While some of the lectures discussed lessons learned from the ENIAC, others focused on the design of its successor, the EDVAC. These lectures influenced the design of future machines built in the United States and the United Kingdom.

During World War II, British engineer F. C. Williams was actively involved in the development of cathode ray tubes (CRTs) used in radar systems. After the war, he decided to put his knowledge to use by figuring out how to use a CRT as a storage device for digital information. In early 1948 a team at the University of Manchester set out to build a small computer that would use a CRT storage device, now called the Williams Tube, to store the program and its data. They called their system the Small-Scale Experimental Machine. The computer successfully executed its first program in 1948. The Small-Scale Experimental Machine was the first

operational, fully electronic computer system that had both program and data stored in its memory.

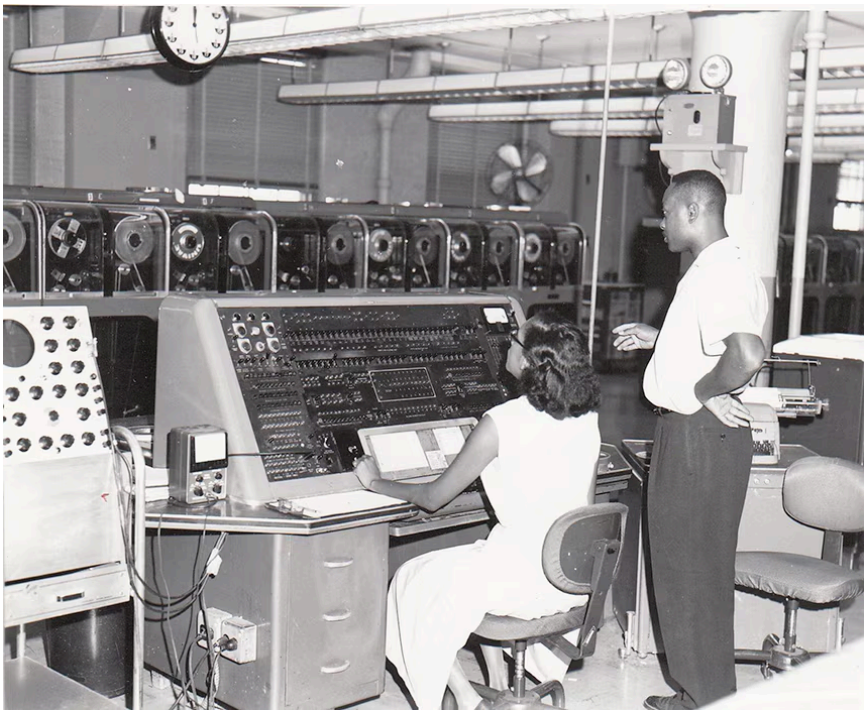
1.2.6 First Commercial Computers

In 1951 the British corporation Ferranti Ltd. introduced the Ferranti Mark 1, the world's first commercial computer. The computer was the direct descendant of research computers constructed at the University of Manchester. Ferranti delivered nine computers between 1951 and 1957, and later Ferranti models boasted a variety of technological breakthroughs, thanks to the company's close association with research undertaken at the University of Manchester and Cambridge University.

After completing work on the ENIAC, Eckert and Mauchly formed their own company to produce a commercial digital computer. The Eckert-Mauchly Computer Corporation signed a preliminary agreement with the National Bureau of Standards (representing the Census Bureau) in 1946 to develop a commercial computer, which they called the UNIVAC, for "universal automatic computer." The project experienced huge cost overruns, and by 1950 the Eckert-Mauchly Computer Corporation was on the brink of

bankruptcy. Remington Rand bought them out and delivered the UNIVAC I to the US Bureau of the Census in 1951 (Figure 1.6) [16].

Figure 1.6



UNIVAC computer at the US Census Bureau with two operators. (Mil image/Alamy Stock Photo)

In a public relations coup, Remington Rand cooperated with CBS to use a UNIVAC computer to predict the outcome of the 1952 presidential election. The events of election night illustrate the tough decisions people can face when computers produce unexpected results.

Adlai Stevenson had led Dwight Eisenhower in polls taken before the election, but less than an hour after voting ended, with just 7 percent of the votes tabulated, the UNIVAC was

predicting Dwight Eisenhower would win the election in a landslide. When CBS correspondent Charles Collingwood asked Remington Rand for the computer's prediction, however, he was given the run-around. The computer's engineers were convinced there was a programming error. For one thing, UNIVAC was predicting that Eisenhower would carry several Southern states, and everybody "knew" that Republican presidential candidates never won in the South. Remington Rand's director of advanced research ordered the engineers to change the programming so the outcome would be closer to what the political pundits expected. An hour later, the reprogrammed computer predicted that Eisenhower would win by only nine electoral votes, and that's what CBS announced. As it turns out, the computer was right and the human "experts" were wrong. Before being reprogrammed, UNIVAC had predicted Eisenhower would win 438 electoral votes to 93 for Stevenson. The official result was a 442–89 victory for Eisenhower [**16**].

In the United States in the early 1950s, the word "UNIVAC" was synonymous with "computer." Remington Rand sold a total of 46 UNIVACs to government agencies, such as the US Air Force, the US Army Map Service, the Atomic Energy Commission, and the US Navy, as well as to large

corporations and public utilities, such as General Electric, Metropolitan Life, US Steel, Du Pont, Franklin Life Insurance, Westinghouse, Pacific Mutual Life Insurance, Sylvania Electric, and Consolidated Edison.

Office automation leader IBM did not enter the commercial computer market until 1953, and its initial products were inferior to the UNIVAC. However, IBM quickly turned the tables on Remington Rand, thanks to a larger base of existing customers, a far superior sales and marketing organization, and a much greater investment in research and development. In 1955 IBM held more than half the market, and by the mid-1960s IBM dominated the computer industry with 65 percent of total sales, compared to 12 percent for number-two computer maker Sperry Rand (the successor to Remington Rand) [**16**]. Many people considered IBM to be a monopoly, and in 1969, the US Department of Justice filed an antitrust suit against IBM, seeking to break it up into smaller companies that would compete with each other. The trial began in 1975 and lasted for more than six years. In 1982, the Department of Justice dropped the lawsuit.

1.2.7 Programming Languages and Time-

Sharing

In the earliest digital computers, every instruction was coded as a long string of 0s and 1s. People immediately began looking for ways to make coding faster and less error-prone. One early improvement was the creation of assembly language, which allowed programmers to work with symbolic representations of the instruction codes. Still, one assembly-language instruction was required for every machine instruction. Programmers wanted fewer, higher-level instructions to generate more machine instructions. In 1951 Frances Holberton, one of the six original ENIAC programmers, created a sortmerge generator for the UNIVAC that took a specification of files to be manipulated and automatically produced the machine program to do the sorting and merging. Building on this work, Grace Murray Hopper, also at Remington Rand, developed the A-0 system that automated the process of linking together subroutines to form the complete machine code [**17**].

Over at IBM, John Backus convinced his superiors of the need for a higher-level programming language for IBM computers. He led the effort to develop the IBM Mathematical Formula Translating System, or FORTRAN. Designed for scientific applications, the first system was

completed in 1957. Many skeptics believed that any "automatic programming" system would generate inefficient machine code compared to hand-coded assembly language, but they were proven wrong: the FORTRAN compiler generated high-quality code. What's more, programmers could write FORTRAN programs 5–20 times faster than the equivalent assembly language programs. Most programmers quickly shifted allegiance from assembly language to FORTRAN. Eventually, other computer manufacturers developed their own FORTRAN compilers, and FORTRAN became an international standard [**18**].

Meanwhile, business-oriented programming languages were also being developed by several computer manufacturers. Grace Murray Hopper specified FLOW-MATIC, an English-like programming language for the UNIVAC. Other manufacturers began to develop their own languages. Customers didn't like incompatible languages, because it meant programs written for one brand of computer had to be rewritten before they could be run on another brand of computer. In 1959 an extremely important customer, the US Department of Defense, brought together a committee to develop a common business-oriented programming language that all manufacturers would support. The committee wrote the specification for COBOL. By requiring manufacturers to

support COBOL in order to get defense contracts, the US Department of Defense helped ensure its widespread adoption [**19**].

In the early 1960s, John Kemeny and Thomas Kurtz at Dartmouth College directed teams of undergraduate students who developed a time-sharing system and an easy-to-learn programming language. The Dartmouth Time-Sharing System (DTSS) gave multiple users the ability to edit and run their programs simultaneously, by dividing the computer's time among all the users. Time-sharing made computers accessible to more people because it allowed the cost of owning and operating a computer system to be divided among a large pool of users who purchased the right to connect to the system [**20**].

The development of BASIC, a simple, easy-to-learn programming language, was another important step toward making computers accessible to a wider audience. Kemeny and Kurtz saw BASIC as a way to teach programming, and soon many other educational institutions began teaching students how to program using Dartmouth BASIC. The language's popularity led computer manufacturers to develop their own versions of BASIC [**20**].

1.2.8 Transistor and Integrated Circuit

Although the British had radar installations at the beginning of World War II, it became clear during the Battle of Britain that their systems had inadequate resolution. The United Kingdom and the United States worked together to develop microwave radar systems capable of locating enemy planes more precisely. Microwave radar required higher-frequency receivers utilizing semiconductors, and in the process of manufacturing microwave radar systems for the war effort, several US companies, including AT&T, greatly improved their ability to create semiconductors [**21**].

AT&T was on the lookout for a new technology to replace the vacuum tube. Its long-distance network relied on vacuum tubes to amplify signals, but the tubes required a lot of power, generated a lot of heat, and burned out like lightbulbs. After the war, AT&T put together a team of Bell Labs scientists, led by Bill Shockley, to develop a semiconductor substitute for the vacuum tube. In 1948 Bell Labs announced the invention of such a device, which they called the **transistor** [**22**].

While most electronics companies ignored the invention of the transistor, Bill Shockley understood its potential. He left Bell Labs and moved to Palo Alto, California, where he founded Shockley Semiconductor in 1956. He hired an exceptional team of engineers and physicists, but many disliked his heavy-handed management style [**22**]. In September 1957, eight of Shockley's most talented employees, including Gordon Moore and Robert Noyce, walked out. The group, soon to be known as the "traitorous eight," founded Fairchild Semiconductor. By this time transistors were being used in a wide variety of devices, from transistor radios to computers. While transistors were far superior to vacuum tubes, they were still too big for some applications. Fairchild Semiconductor set out to produce a single semiconductor device containing transistors, capacitors, and resistors; in other words, an **integrated circuit**. Another firm, Texas Instruments, was on the same mission. Today Robert Noyce of Fairchild Semiconductor and Jack Kilby of Texas Instruments are credited for independently inventing the integrated circuit [**23**].

The Cold War between the United States and the Soviet Union played an important role in advancing integrated circuit technology. US engineers developing the Minuteman II ballistic missile in the early 1960s decided to use integrated

circuits to improve the processing speed of its guidance computer. The Minuteman II program was the single largest consumer of integrated circuits in the United States between 1962 and 1965, representing about 20 percent of total sales. During these years companies learned how to make rugged, reliable integrated circuits [**11**]. They also continued to shrink the components within the integrated circuits, leading to an exponential increase in their power. Gordon Moore noted this trend in a 1965 paper and predicted it would continue. Today **Moore's law** refers to the phenomenon that the number of transistors in the most powerful integrated circuits doubles roughly every two years.

1.2.9 IBM System/360

The integrated circuit made possible the construction of much more powerful and reliable computers. The 1960s was the era of mainframe computers—large computers designed to serve the data-processing needs of large businesses. Mainframe computers enabled enterprises to centralize all their data-processing applications in a single system. As we have seen, by this time IBM dominated the mainframe market in the United States.

In 1964 IBM unveiled the System/360, a series of 19 compatible computers with varying levels of computing speed and memory capacity (Figure 1.7). Because the systems were software compatible, a business could upgrade its computer without having to rewrite its application programs. This feature was important, because by the 1960s companies were making much larger investments in software.

Figure 1.7

In the 1960s, IBM dominated the mainframe computer market in the United States.

(H. Armstrong Roberts/ClassicStock/Alamy Stock Photo)

1.2.10 Microprocessor

In 1968 Robert Noyce and Gordon Moore left Fairchild Semiconductor to found another semiconductor manufacturing company, which they named Intel. A year later Japanese calculator manufacturer Busicom approached Intel about designing 12 custom chips for use in a new scientific calculator. Intel agreed to provide the chips and assigned responsibility for the project to Marcian "Ted" Hoff. After reviewing the project, Hoff suggested that it was not in Intel's best interest to manufacture a custom chip for every customer. As an alternative, he suggested that Intel create a general-purpose chip that could be programmed to perform a wide variety of tasks. Each customer could then program the chip to meet its particular needs. Intel and Busicom agreed to the plan, which reduced the required number of chips for Busicom's calculator from 12 to 4. A year of development by Ted Hoff, Stanley Mazor, and Federico Faggin led to the release of the Intel 4004, the world's first **microprocessor**. Inside the 1/8-inch × 1/6-inch chip were 2,300 transistors, giving the Intel 4004 the same computing power as the ENIAC, which had occupied 3,000 cubic feet.

Microprocessors made it possible to integrate computers into everyday devices. Today we're surrounded by devices containing microprocessors: smartphones, streaming media

players, smart speakers with voice-controlled personal assistants, learning thermostats, video doorbells, augmented reality glasses, self-driving cars, and much more. The highest-profile use of microprocessors, however, is in personal computers.

1.2.11 Personal Computer

During the Vietnam conflict in the late 1960s and early 1970s, the area around San Francisco was home to a significant counterculture, including a large number of antiwar and antiestablishment activists. The do-it-yourself idealism of the power-to-the-people movement intersected with advances in computer technology in a variety of ways, including the *Whole Earth Catalog*, the People's Computer Company, and the Homebrew Computer Club [**24**].

The *Whole Earth Catalog*, first published in 1968, was, in the words of Steve Jobs, "sort of like Google in paperback form" [**25**] —an effort to pull together in a single large volume lists of helpful tools, in this case for the creation of a more just and environmentally sensitive society. The definition of "tools" was broad; the catalog's lists included books, classes, garden tools, camping equipment, and (in later issues) early personal computers. "With the *Whole*

Earth Catalog, Stewart Brand offered a generation of computer engineers and programmers an alternative vision of technology as a tool for individual and collective transformation" [**26**, p. 104].

The People's Computer Company was a not-for-profit corporation dedicated to educating people on how to use computers. One of its activities was publishing a newspaper. The cover of the first issue read: "Computers are mostly used against people instead of for people, used to control people instead of to free them, time to change all that—we need a People's Computer Company" [**27**]. Typical issues contained programming tips and the source code to programs, particularly educational games written in BASIC. The newspaper's publisher, Bob Albrecht, said, "I was heavily influenced by the *Whole Earth Catalog*. I wanted to give away ideas" [**26**, p. 114]. The People's Computer Company also set up the People's Computer Center in a strip mall in Menlo Park, California. The center allowed people to rent teletype terminals connected to a timeshared computer. A large number of teenagers were drawn to computing through Friday evening game-playing sessions. Many users wrote their own programs, and the center promoted a culture in which computer enthusiasts freely shared software with each other.

In 1975 the Homebrew Computer Club, an outgrowth of the People's Computer Company, became a meeting place for hobbyists interested in building personal computers out of microprocessors. A company in Albuquerque, New Mexico, called MITS had recently begun shipping the Altair 8800 personal computer, and during the first few Homebrew Computer Club meetings, members showed off various enhancements to the Altair 8800. Progress was frustratingly slow, however, due to the lack of a higher-level programming language.

Three months after the establishment of the Homebrew Computer Club, MITS representatives visited Palo Alto, California, to demonstrate the Altair 8800 and the BASIC interpreter created by Paul Allen and Bill Gates, who had a tiny company called Micro-Soft. The audience in the hotel conference room was far larger than expected, and during the overcrowded and chaotic meeting somebody acquired a paper tape containing the source code to Altair BASIC. More than 70 copies of the tape were handed out at the next meeting of the Homebrew Computer Club. After that, free copies of the interpreter proliferated. Some hobbyists felt that the asking price of $500 for the BASIC interpreter was too

high, considering that the Altair computer itself cost only $395 as a kit or $495 preassembled [**24**].

Bill Gates responded by writing "An Open Letter to Hobbyists," which was reprinted in a variety of publications. In the letter he asserted that less than 10 percent of all Altair owners had purchased BASIC, even though far more people than that were using it. According to Gates, the royalties Micro-Soft had received from Altair BASIC made the time spent on the software worth less than $2 an hour. He wrote, "Nothing would please me more than being able to hire 10 programmers and deluge the hobby market with good software," but the theft of software created "very little incentive" for his company to release new products [**24**].

The controversy over Altair BASIC did not slow the pace of innovations. Hobbyists wanted to do more than flip the toggle switches and watch the lights blink on the Altair 8800. Steve Wozniak, a computer engineer at Hewlett-Packard, created a more powerful personal computer that supported keyboard input and television monitor output. Wozniak's goal was to make a machine for himself and to impress other members of the Homebrew Computer Club, but his friend Steve Jobs thought of a few improvements and convinced Wozniak they should go into business (Figure 1.8). They

raised $1,300 by selling Jobs's Volkswagen van and Wozniak's Hewlett-Packard scientific calculator, launching Apple Computer. Although the company sold only 200 Apple I computers, its next product, the Apple II, became one of the most popular personal computers of all time.

Figure 1.8

Steve Jobs (right) convinced Steve Wozniak (left) they should go into business selling the personal computer Wozniak designed. They named their company Apple Computer.

(Kimberly White/Reuters)

By the end of the 1970s, many companies, including Apple Computer and Tandy, were producing personal computers. While hundreds of thousands of people bought personal computers for home use, businesses were reluctant to move to the new computer platform. However, two significant

developments made personal computers more attractive to businesses.

The first development was the computer spreadsheet program. For decades firms had used spreadsheets to make financial predictions. Manually computing spreadsheets was monotonous and error-prone, since changing a value in a single cell could require updating many other cells. In the fall of 1979, Dan Bricklin and Bob Frankston released their program, called VisiCalc, for the Apple II. VisiCalc's labor-saving potential was obvious to businesses. After a slow start, it quickly became one of the most popular application programs for personal computers. Sales of the Apple II computer increased significantly after the introduction of VisiCalc.

The second development was the release of the IBM PC in 1981. The IBM name exuded reliability and respectability, making it easier for companies to make the move to desktop systems for their employees. As the saying went, "Nobody ever got fired for buying from IBM." In contrast to the approach taken by Apple Computer, IBM decided to make its PC an open architecture, meaning the system was built from off-the-shelf parts and other companies could manufacture "clones" with the same functionality. This decision helped to

make the IBM PC the dominant personal computer architecture.

The success of IBM-compatible PCs fueled the growth of Microsoft. In 1980 IBM contracted with Microsoft to provide the DOS operating system for the IBM PC. Microsoft let IBM have DOS for practically nothing, but in return IBM gave Microsoft the right to collect royalties from other companies manufacturing PC-compatible computers. Microsoft profited handsomely from this arrangement when PC-compatibles manufactured by other companies gained more than 80 percent of the PC market [28].

1.3 Milestones in Networking

In the early nineteenth century, the United States fell far behind Europe in networking technology. The French had begun constructing a network of telegraph towers in the 1790s, and 40 years later there were towers all over the European continent (Figure 1.9). At the top of each tower was a pair of semaphores. Operators raised and lowered the semaphores; each pattern corresponded to a letter or symbol. A message initiated at one tower would be seen by another tower within viewing distance. The receiving tower would then repeat the message for the next tower in the network, and so on. This optical telegraph system could transmit messages at the impressive rate of about 350 miles per hour when skies were clear.

Figure 1.9

In 1837 Congress asked for proposals to create a telegraph system between New York and New Orleans. It received one proposal based on proven European technology. Samuel Morse submitted a radically different proposal. He suggested constructing a telegraph system that used electricity to communicate the signals. Let's step back and review some of the key discoveries and inventions that enabled Morse to make his dramatic proposal.

1.3.1 Electricity and Electromagnetism

Amber is a hard, translucent, yellowish-brown fossil resin often used to make beads and other ornamental items. About

2,600 years ago the Greeks discovered that if you rub amber, it becomes charged with a force enabling it to attract light objects such as feathers and dried leaves. The Greek word for amber is *ηλεκτρων* (electron). Our word "electric" literally means "like amber."

For more than 2,000 years, amber's ability to attract other materials was seen as a curiosity with no practical value, but in the seventeenth and eighteenth centuries scientists began to study electricity in earnest. Alessandro Volta, a professor of physics at the University of Pavia, made a key breakthrough when he discovered that electricity could be generated chemically. He produced an electric current by submerging two different metals close to each other in an acid. In 1799 Volta used this principle to create the world's first battery. Volta's battery produced an electric charge more than 1,000 times as powerful as that produced by rubbing amber. Scientists soon put this power to practical use.

In 1820 Danish physicist Christian Oersted discovered that an electric current creates a magnetic field. Five years later British electrician William Sturgeon constructed an electromagnet by coiling wire around a horseshoe-shaped piece of iron. When he ran an electric current through the coil, the iron became magnetized. Sturgeon showed how a

single battery was capable of producing a charge strong enough to pick up a nine-pound metal object.

In 1830 US professor Joseph Henry rigged up an experiment that showed how a telegraph machine could work. He strung a mile of wire around the walls of his classroom at the Albany Academy. At one end he placed a battery; at the other end he connected an electromagnet, a pivoting metal bar, and a bell. When Henry connected the battery, the electromagnet attracted the metal bar, causing it to ring the bell. Disconnecting the battery allowed the bar to return to its original position. In this way he could produce a series of rings.

1.3.2 Telegraph

Samuel Morse, a professor of arts and design at New York University, worked on the idea of a telegraph during most of the 1830s, and in 1838 he patented his design of a telegraph machine. The US Congress did not approve Morse's proposal in 1837 to construct a New York–to–New Orleans telegraph system, but it did not fund any of the other proposals either. Morse persisted with his lobbying, and in 1843 Congress appropriated $30,000 to Morse for the construction of a 40-

mile telegraph line between Washington, DC, and Baltimore, Maryland.

On May 1, 1844, the Whig party convention in Baltimore nominated Henry Clay for president. The telegraph line had been completed to Annapolis Junction at that time. A courier hand-carried a message about Clay's nomination from Baltimore to Annapolis Junction, where it was telegraphed to Washington. This was the first news reported via telegraph. The line officially opened on May 24. Morse, seated in the old Supreme Court chamber inside the US Capitol, sent his partner in Baltimore a verse from the Bible: "What hath God wrought?"

The value of the telegraph was immediately apparent, and the number of telegraph lines quickly increased. By 1846 telegraph lines connected Washington, Baltimore, Philadelphia, New York, Buffalo, and Boston. In 1850 twenty different companies operated 12,000 miles of telegraph lines. The first transcontinental telegraph line was completed in 1861, putting the Pony Express out of business (Figure 1.10). The telegraph was the sole method of rapid long-distance communication until 1877. By this time the United States was networked by more than 200,000 miles of telegraph wire [29].

Figure 1.10

Pony Express riders lost their jobs when the US transcontinental telegraph line was completed in 1861.

(North Wind Picture Archives/Alamy Stock Photo)

The telegraph was a versatile tool, and people kept finding new applications for it. For example, by 1870 fire-alarm telegraphs were in use in 75 major cities in the United States. New York City alone had 600 fire-alarm telegraphs. When a person pulled the lever of the alarm box, it automatically transmitted a message identifying its location to a fire station. These devices greatly improved the ability of fire departments to dispatch equipment quickly to the correct location [29].

1.3.3 Telephone

Alexander Graham Bell was born in Edinburgh, Scotland, into a family focused on elocution and the correction of speech. His mother was almost completely deaf. Bell was educated to follow in the same career path as his father and grandfather, and he became a teacher of deaf students. Later, he married a deaf woman.

Bell pursued inventing as a means of achieving financial independence. At first he focused on making improvements to the telegraph. A significant problem with early telegraph systems was that a single wire could transmit only one message at a time. If multiple messages could be sent simultaneously along the same wire, communication delays would be reduced, and the value of the entire system would increase.

Bell's solution to this problem was called a harmonic or musical telegraph. If you imagine hearing Morse code, it's obvious that all of the dots and dashes are the same note played for a shorter or longer period of time. The harmonic telegraph assigned a different note (different sound frequency) to each message. At the receiving end, different receivers could be tuned to respond to different notes, as you can tune your radio to hear only what is broadcast by a

particular station. In this way, a single telegraph wire could carry multiple messages simultaneously.

Bell knew that the human voice is made up of sounds at many different frequencies. From his work on the harmonic telegraph, he speculated that it should be possible to capture and transmit human voice over a wire. He and Thomas A. Watson succeeded in transmitting speech electronically in 1876. Soon after, they commercialized their invention.

Nearly all early telephones were installed in businesses. Leasing a telephone was expensive, and most people focused on its commercial value rather than its social value. However, the number of phones placed in homes increased rapidly in the 1890s, after Bell's first patent expired.

Once telephones were placed in the home, the traditional boundaries between private family life and public business life became blurred. People enjoyed being able to conduct business transactions from the privacy of their home, but they also found that a ringing telephone could be an unwelcome interruption [30].

Another consequence of the telephone was that it eroded traditional social hierarchies. An 1897 issue of *Western Electrician* reports that Governor Chauncey Depew of New

York was receiving unwanted phone calls from ordinary citizens: “Every time they see anything about him in the newspapers, they call and tell him what a ‘fine letter he wrote’ or ‘what a lovely speech he made,’ or ask if this or that report is true; and all this from people who, if they came to his office, would probably never say more than ‘Good morning’” [**31**].

People also worried about the loss of privacy brought about by the telephone. In 1877 the *New York Times* reported that telephone workers responsible for operating an early system in Providence, Rhode Island, overheard many confidential conversations. The writer fretted that telephone eavesdropping would make it dangerous for anyone in Providence to accept nomination for public office [**30**].

The telephone enabled the creation of the first “online” communities. In rural areas the most common form of phone service was the party line: a single circuit connecting multiple phones to the telephone exchange. Party lines enabled farmers to gather by their phones every evening to talk about the weather and exchange gossip [**32**].

The power of this new medium was demonstrated in the Bryan/McKinley presidential election of 1896. For the first time, presidential election returns were transmitted directly

into people's homes. "Thousands sat with their ear glued to the receiver the whole night long, hypnotized by the possibilities unfolding to them for the first time" [33].

1.3.4 Typewriter and Teletype

For hundreds of years people dreamed of a device that would allow an individual to produce a document that looked as if it had been typeset, but the dream was not realized until 1867, when Christopher Sholes, Carlos Glidden, and Samuel Soule patented the first typewriter. In late 1873 Remington & Sons Company, famous for guns and sewing machines, produced the first commercial typewriter. It was difficult to use and was not well received; Remington & Co. sold only 5,000 machines in the first five years. However, the typewriter did get the attention of Mark Twain, who used it to produce *Tom Sawyer*, which may have been the world's first typewritten manuscript. By 1890 more reliable typewriters were being produced, and the typewriter became a common piece of office equipment [34].

In 1908 Charles and Howard Krum succeeded in testing an experimental machine that allowed a modified typewriter to print a message transmitted over a telegraph line. They called

their invention the teletype. During the 1920s, news organizations began using teletype machines to transmit stories between distant offices, and Wall Street firms began sending records of stock transactions over teletypes.

1.3.5 Radio

Earlier we described how the experiments of Oersted, Sturgeon, and Henry led to the development of the electromagnet and the telegraph. The connection between electricity and magnetism remained mysterious, however, until Scottish physicist James Clerk Maxwell published a mathematical theory demonstrating their relationship. This theory predicted the existence of an electromagnetic wave spreading with the velocity of light. It also predicted that light itself was an electromagnetic phenomenon. In 1885 Heinrich Hertz successfully generated electromagnetic waves, proving the correctness of Maxwell's theory.

Guglielmo Marconi put Hertz's discovery to practical use by successfully transmitting radio signals in the hills outside Bologna, Italy, in 1895. Unable to attract the attention of the Italian government, he took his invention to England, where he founded the Marconi Wireless Telegraph Company. The name of the company reflects Marconi's concept of how his

invention would be used. To Marconi, radio, or "wireless," was a superior way to transmit telegraph messages.

David Sarnoff emigrated from Russia to the United States with his family when he was nine. When he had completed school, he landed a position with the Marconi Wireless Telegraph Company. In 1912 Sarnoff made a name for himself when his post—the wireless station at the Wanamaker department store in New York City—relayed news about the sinking of the *Titanic*. Four years later, Sarnoff suggested the use of radio as an entertainment device, writing: "I have in mind a plan of development which would make radio a household utility in the same sense as the piano or phonograph. . . . The receiver can be designed in the form of a simple music box . . . [which] can be placed in the parlor or living room" [35]. In two decades, Sarnoff's vision had become a reality.

The power of radio as a medium of mass communication was demonstrated on the evening of October 30, 1938 (the night before Halloween). From CBS Radio Studio One in New York City, Orson Welles and the Mercury Theater put on a one-hour dramatization of H. G. Wells's *War of the Worlds*. To increase suspense, the play was performed as a series of news bulletins interrupting a concert of dance music. These

bulletins described events occurring on a farm near Grovers Mill, New Jersey. Many listeners panicked. “People packed the roads, hid in cellars, loaded guns, even wrapped their heads in wet towels as protection from Martian poison gas, oblivious to the fact that they were acting out the role of the panic-stricken public that actually belonged in a radio play” [36].

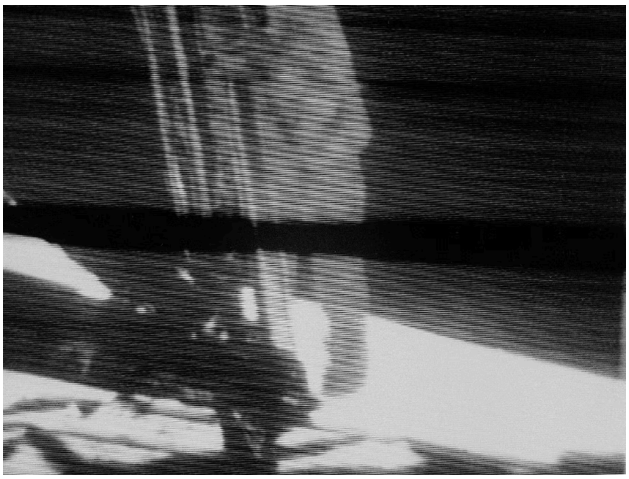
1.3.6 Television

Broadcasting video over a wire began in 1884 with the invention of an electromechanical television by Paul Nipkow, but the first completely electronic television transmission was made in 1927 by Philo Farnsworth. Millions of Americans were formally introduced to the television at the 1939 World’s Fair held in New York City, which had as its theme “The World of Tomorrow.” Since an early retail television set cost about as much as an automobile, televisions remained a rarity in US households until the 1950s, when prices fell dramatically.

Television’s ability to send a message around the world was demonstrated in July 1969. Hundreds of millions of people watched on live TV as US astronaut Neil Armstrong stepped

from the lunar module onto the surface of the Moon (Figure 1.11).

Figure 1.11



On July 20, 1969, television images of Neil Armstrong walking on the Moon were broadcast to hundreds of millions of viewers around the world. (Courtesy of NASA)

Television has created many opportunities for "news junkies" to get their fixes. The major commercial broadcast television networks have been supplemented by Fox, CNN, and other cable news organizations as well as a myriad of Web sites. The various organizations compete with one another to be the first to break news stories. Increasingly, the media have turned to computer technology to help them provide information to the public. Sometimes this has led to embarrassing mistakes, as in the 2000 US presidential election.

At about 7:50 p.m. on the evening of Tuesday, November 7, 2000, before the polls had even closed in the Florida panhandle, the major networks began announcing that Al Gore would be the winner in Florida. Based on the expected result of the Florida election, the networks went on to predict —while people were still voting in the Western states—that Al Gore would be the next president of the United States.

You might be wondering how it is possible to predict the outcome of an election before everyone has voted. In a practice known as exit polling, a company called Voter News Service questions people leaving polling places. It combines the information it collects with early returns to predict the outcome of elections. Since 1988 the television networks have relied upon the Voter News Service to provide them with exit polling results.

As it turns out, Voter News Service's prediction was wrong. More than a month after the election, after a series of recounts and court decisions, George W. Bush was declared the victor in Florida. With Florida's electoral votes in hand, Bush won the presidency.

1.3.7 Remote Computing

Working at his kitchen table in 1937, Bell Labs researcher George Stibitz built a binary adder out of telephone relays, batteries, flashlight bulbs, tin strips, and wire. He took his invention back to Bell Labs and enlisted the help of Samuel Williams. Over the next two years they built the Complex Number Calculator, an electromechanical system that would add, subtract, multiply, and divide complex numbers.

Stibitz's next action is what sets him apart from other computer pioneers. He made a teletype machine the input/output device for the Complex Number Calculator. With this innovation, he did not have to be in the same room as the calculator to use it; he could operate it remotely.

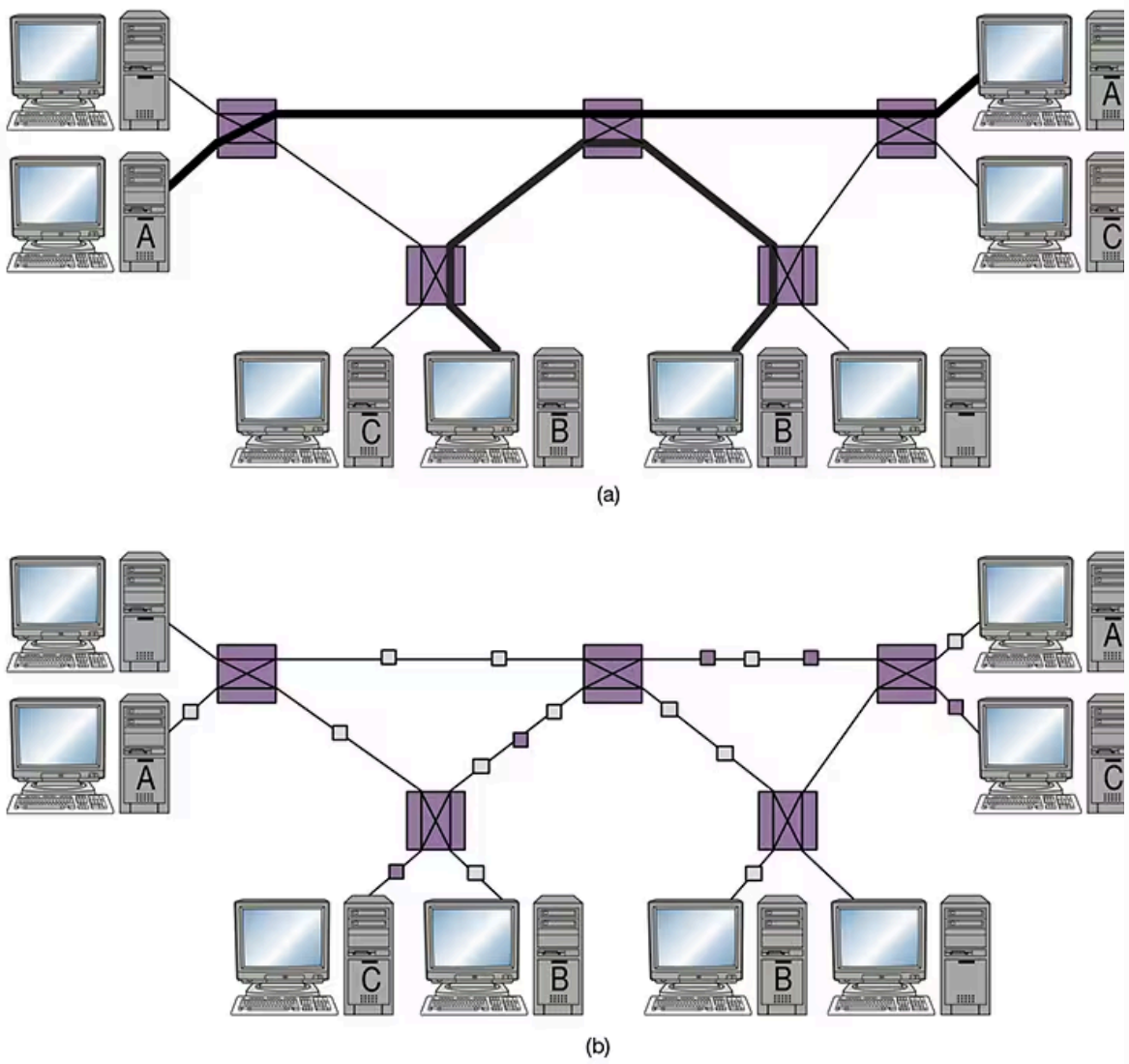
In 1940 Stibitz demonstrated remote computing to members of the American Mathematical Society who were meeting at Dartmouth College in New Hampshire. He typed numbers into the teletype, which transmitted the data 250 miles to the calculator in New York City. After the calculator had computed the answer, it transmitted the data back to the teletype, which printed the result.

1.3.8 ARPANET

In reaction to the launch of Sputnik by the Soviet Union in 1957, the Department of Defense created the Advanced Research Projects Agency (ARPA). ARPA funded research and development at prominent universities. The agency's first director, J. C. R. Licklider, imagined a "galactic network"—a global computer network that would facilitate the exchange of programs and data.[1] This view of the computer as a device to improve communication was in stark contrast to the mind-set of computer manufacturers, which continued to think of computers as number-crunching machines.

Conventional circuit-switched telephone networks were not a good foundation upon which to build a global computer network (Figure 1.12a). Between 1961 and 1967, three research teams independently came up with an alternative to circuit-switched networks. These teams were led by Donald Davies and Roger Scantlebury at NPL in England, Paul Baran at RAND, and Leonard Kleinrock at MIT. Eventually, the new design came to be called a packet-switched network (Figure 1.12b).

Figure 1.12



Comparison of circuit-switched networking and packet-switched networking. (a) In a **circuit-switched network**, a single physical connection is established between the two ends. The physical connection cannot be shared. In this illustration, one circuit links the two computers labeled A, and another circuit links the two computers labeled B. The computers labeled C may not communicate at this time, because no circu can be established. (b) In a **packet-switched network**, a message is divided into small bundles of data called packets. Every packet has the address of the computer where it should be routed. If there is more than

In 1967 ARPA initiated the design and construction of the ARPANET. Fear of a nuclear attack led to the crucially important design decision that the network should be decentralized. In other words, the loss of any single computer

or communication link would not prevent the rest of the network from working. Every computer on the network would have the ability to make decisions about how message traffic should be routed. Packet-switched networks met this condition; circuit-switched networks did not.

BBN in Boston was responsible for the Interface Message Processor (IMP) that connected a computer to the telephone network. In 1969 BBN delivered its first four IMPs to UCLA, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah.

1.3.9 Email

During the earliest years of ARPANET, the networked computers could transfer programs and data only. ARPANET users still relied upon the telephone for personal communications. In March 1972, Ray Tomlinson at BBN wrote the first software enabling email messages to be sent and received by ARPANET computers. A few months later, Lawrence Roberts created the first “killer app” for the network: an email utility that gave individuals the ability to list their email messages, selectively read them, reply to them, forward them to others, and save them. Email quickly became the most popular network application.

Email is now one of the most important communication technologies on the planet. More than 350 billion email messages are sent each day.

1.3.10 Internet

ARPA researchers anticipated the need to connect the ARPANET with other networks based on different designs. Robert Kahn developed the concept of open architecture networking, in which individual networks could be quite different as long as they shared a common "internetworking architecture." Vinton Cerf and Robert Kahn designed the TCP/IP protocol that would support open architecture networking [38]. TCP (Transmission Control Protocol) is responsible for dividing a message into packets at the sending computer and reassembling the packets at the receiving computer. IP (Internet Protocol) is the set of rules used to route data from computer to computer. The **Internet** is the network of networks that communicate using TCP/IP. You could call January 1, 1983, the birth date of the Internet, because that was the date on which all ARPANET hosts converted to TCP/IP.

1.3.11 NSFNET

The National Science Foundation (NSF) in the United States saw the importance of networking to the academic community. It created a TCP/IP–based network called NSFNET, and it provided grants to universities to join the NSFNET. These grants encouraged broad participation by stipulating that universities would have to make their Internet connections available to all qualified users. The NSFNET consisted of regional networks connected by the NSFNET backbone.

The NSF encouraged the universities participating in regional networks to reduce their network subscription costs by finding commercial customers for the networks. At the same time, the NSF banned commercial traffic on the NSFNET backbone. These policies stimulated private companies to create commercial, long-distance Internet connections in the United States. In April 1995 the NSF ceased funding the NSFNET backbone. Commercial network providers, well established by this time, took over the task of supplying long-distance Internet connections in the United States.

1.3.12 Broadband

The term **broadband** refers to a high-speed Internet connection. Broadband connections make feasible the

transfer of large files, such as those containing images, music, and video. The growth of file swapping among Internet users and music and video streaming has paralleled the growth of broadband connections.

Typical broadband speeds vary widely among high-income, industrialized countries. The world broadband leaders are Chile, with a median download speed of 216 megabits per second; China, at 215 megabits per second; and Singapore, at 214 megabits per second. The United States ranks sixth in the world, with an average broadband speed of 189 megabits per second [39].

1.3.13 Wireless Networks

Cell phones, also known as mobile phones, allow telephone calls to be made over radio links. The first cell phone, demonstrated by Motorola in 1973, was quite large and weighed two and a half pounds. Advances in integrated circuits and other technologies have allowed companies to shrink the size and weight of cell phones substantially while greatly increasing their capabilities. Modern **smartphones**, such as the one shown in Figure 1.1, weigh just a few ounces and support a wide variety of services in addition to voice

communication, including text messaging, email, and Internet access.

The social impact of cellular networks has been dramatic, particularly in countries with previously limited infrastructure. People living in areas never reached by wired telephone service now have the ability to communicate with others and access the Internet. Three-quarters of the people in the world aged 10 and older now own a cell phone [**40**].

In 1993 Henrik Sjödin proposed the development of public-access wireless local area networks. Today wireless Internet access points, or **hotspots**, are commonplace at coffee shops, libraries, airports, university campuses, and other public places where people gather. Computers and other electronic devices within range of the hotspot communicate with the hotspot using radio waves. Most hotspots use a technology known as Wi-Fi.

1.3.14 Cloud Computing

Cloud computing refers to the utilization of remote computing resources over the Internet; the term comes from the tradition of representing networks as clouds in technical diagrams [**41**, **42**].

Several important technological breakthroughs made cloud computing possible: high-speed networks; high-performance, low-cost microprocessors; low cost of storage devices; and **virtualization**—software that enables a single physical computer to emulate many virtual computing devices.

Providers of cloud computing services have assembled massive data centers that achieve an economy of scale, allowing the providers to lease computational resources to customers at an attractive price. Customers have tremendous flexibility to choose the specifications of the virtual machines they are leasing as well as the number of these machines they wish to employ for their computation.

Many kinds of service are available through cloud computing, including software as a service and infrastructure as a service. Software as a service means the use of remote computing resources to deliver applications to the user, typically through a Web browser. Microsoft's Office 365 is an example of software as a service. Infrastructure as a service allows customers to utilize remote storage and computational capabilities on a pay-as-you-go basis. The most popular providers of infrastructure as a service are Amazon Web Services, Microsoft Azure, Google Cloud Platform, and IBM Cloud [**43**].

ıe primary source document for this description of the evolution of the Inter
A Brief History of the Internet by Barry M. Leiner et al. [**37**].

1.4 Milestones in Information Storage and Retrieval

The previous two sections surveyed technological developments related to manipulating and transmitting information, respectively. This section focuses on the development of technologies to store and retrieve information.

1.4.1 Greek Alphabet

As civilizations expanded around 6,000 years ago, writing systems were developed to allow the recording and communication of various types of information, such as laws and financial records. There are three general types of writing systems. In a logography each character represents a word, in a syllabary each character represents a syllable, and in an alphabet each character represents a phoneme.

In the eighth century BC, the Greeks developed the first true alphabet: an alphabet representing vowel sounds as well as

consonant sounds. Compared with earlier writing systems developed in Mesopotamia and Egypt, the 24-letter Greek alphabet was a simple, efficient way of transforming the spoken word into written form, and it marked an important milestone on the journey from an oral culture to a written culture. The English alphabet we use today is a direct descendant of the alphabet used by the ancient Greeks [**44**].

1.4.2 Codex and Paper

Two thousand years ago, important information was recorded on papyrus scrolls wrapped around wooden rods. Papyrus had to be stored this way to keep from breaking apart. Even so, the ends of papyrus scrolls tended to fall off.

The development of the codex was a significant advance in information storage and retrieval technology. A codex was made up of rectangular pages sewn together on one side. These pages were made out of sheepskin (parchment) or calfskin (vellum). The codex was superior to papyrus in two ways. First, the codex was much more durable than a papyrus roll. Second, since it was divided into pages, the codex made it much easier for readers to find a particular passage: they could simply flip to the desired page.

Between the second and fourth centuries, the codex gradually replaced the scroll as the most popular method of recording important information. The Church accelerated the transition by insisting that all sacred texts be recorded in codices, to distinguish them from Hebrew scriptures kept on scrolls.

After the fall of the Roman Empire, Irish monks preserved Western culture by copying Greco-Roman and Judeo-Christian texts into codices [45]. Centuries later, most codices were produced using a process of wood engraving. A craftsman would take a block of wood and laboriously chisel away the background for a portion of a page, leaving the letters and illustrations raised. When all the wooden blocks for a page were carved, they would be fastened together. After the surface was inked, a blank page would be printed by pressing the blocks down on the inked surface.

The invention of paper is credited to Cai Lun of China in the early second century. In the late Middle Ages, European explorers learned and brought back from China the technology for manufacturing paper in mass quantities. By the fifteenth century, paper gradually began to replace parchment in less expensive European codices.

1.4.3 Gutenberg's Printing Press

In 1436 Johannes Gutenberg began work on a printing press that would imprint pages using movable metal type rather than wood blocks, and in 1455 work was completed on Gutenberg's famous "42-Line Bible." Soon other printers were using the same technology to produce codices. The principal customer of these publishers was the Church. Hence most early publications were religious books and pamphlets. The number of books in circulation rose as their price dropped, and the widespread availability of printed material led to an increase in the literacy rate.

The printing press proved itself to be a powerful tool for mass communication during the Reformation. Martin Luther did more than nail his 95 theses to the door of a church—he published them. Between 1517 and 1520, more than 300,000 copies of Martin Luther's publications were sold [**46**]. In the next 50 years, the number of religious tracts produced by Protestant reformers would outnumber those of their Catholic opponents by a factor of 10 to 1.

1.4.4 Newspapers

The printing press made possible the establishment of newspapers. Newspapers provided an important new way for private citizens to get their points of view heard. A free press serves as a powerful counterweight to government and its desire to manage the flow of information. It is not surprising, then, that there is a long history of government censorship or suppression of newspapers.

The first English-language newspaper appeared in Great Britain in the 1600s. Throughout most of the seventeenth century the government controlled the press by licensing approved newspapers and suppressing the rest. However, in 1695 Parliament declined to renew the Licensing Act, paving the way for a free press in England.

In North America, newspapers helped to unify the colonies. As colonists read newspapers published in other colonies, they came to realize what values and concerns they shared with other colonists up and down the Atlantic seaboard. In this way newspapers played an important role in swaying public opinion toward favoring independence from Great Britain.

1.4.5 Hypertext

The July 1945 issue of the *Atlantic Monthly* contained a visionary paper, "As We May Think," written by Vannevar Bush, who had served as director of the Office of Scientific Research and Development in World War II. In the paper Bush noted, "The world has arrived at an age of cheap complex devices of great reliability; and something is bound to come of it" [**47**, p. 102]. He described many ways in which technology can solve important problems. One of the problems he focused on was that of information retrieval. He pointed out how difficult it is for scientists to keep up with all the research results that are being published, especially when indexing systems do not lend themselves to exposing the relationships among documents. Bush noted that the human mind doesn't work by indexing. Instead, our memories are associative. When we think of one thing, other related memories awaken in our minds. He suggested that a machine could simulate, to some degree, the mind's ability to make associations between pieces of information. He gave a description for the Memex, an information retrieval system equipped with "a provision whereby any item may be caused at will to select immediately and automatically another" [**47**, p. 107].

Ted Nelson was raised by his grandparents in Greenwich Village, New York. He was a graduate student studying sociology at Harvard when he took his first computer class. There he discovered that "everything everyone was saying about computers was a lie. It was up to me to design the literature of the future" [48, p. 134]. In 1965 Nelson coined the word hypertext, which refers to a linked network of nodes containing information. The links allow readers to visit the nodes in a nonlinear fashion [49]. The proposed system had much in common with Bush's proposal for Memex. In 1967 Nelson proposed the creation of a system called Xanadu, a worldwide network of connected literature. Despite decades of work and a $5 million investment from Autodesk, the system was never completed [48].

1.4.6 Graphical User Interface

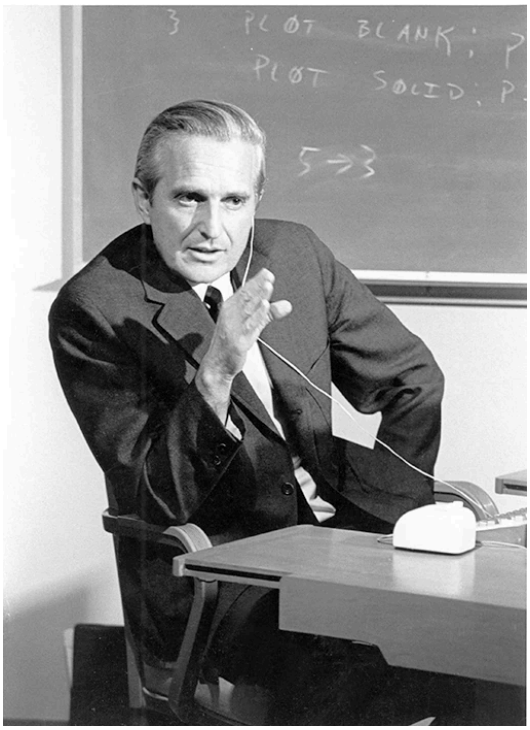
Douglas Engelbart grew up on a dairy farm in Oregon. After graduating from high school, he attended Oregon State College, but his electrical engineering studies were interrupted by World War II. While he was stationed in the Philippines, he worked with radar and read "As We May Think" by Vannevar Bush. These two experiences shaped his

views about the potential of computing. When his military service ended, he completed his degree at OSC and took a job at Ames Laboratory, but soon began wondering, “How can my career maximize my contribution to mankind?” [50]. Engelbart decided to return to school and completed a PhD in electrical engineering from the University of California, Berkeley, in 1955. He joined the Stanford Research Institute, where he set out to use the power of the computer to augment human intellect.

In the 1950s and 1960s, people submitted computer jobs in the form of decks of punch cards and often waited hours for them to run. Computer output was typically pages full of numbers that programmers would laboriously examine. Engelbart wondered why people couldn’t interact directly with computers and view the output on a CRT, like radar images. He created a research lab called the Augmentation Research Center. This lab developed a hypermedia and groupware system called NLS (oNLine System). Engelbart invented several new input devices, including the computer mouse. In 1968 at the Fall Joint Computer Conference in San Francisco, he gave a 90-minute demonstration of NLS that included a video display divided into windows, email, use of a mouse to direct a cursor, and live videoconferencing with staff members 30 miles away (Figure 1.13). Engelbart’s

presentation is still called “the mother of all demos.” Paul Saffo said, “It was like a UFO landing on the White House lawn.” The presentation was so far ahead of its time that some audience members thought it was a hoax [51]. Others thought Engelbart’s ideas were completely impractical, noting that he was treating a computer as if it were for his personal use.

Figure 1.13



Douglas Engelbart rehearses for his presentation at the 1968 Fall Joint Computer Conference. It is still called “the mother of all demos.” (PVDE/Bridgeman Images)

Alan Kay saw Engelbart’s demo, understood the ramifications of NLS, and was eager to take the next step. In 1970 he became one of the founding members of Xerox Palo Alto Research Center (PARC), a new facility dedicated to

performing research into digital technology. The research team created the Alto, a small minicomputer designed to be used by a single person. The Alto incorporated a bitmapped display, a keyboard, and a mouse. Kay played a leading role in developing the Alto's graphical user interface that responded to the point, click, and drag operations of a mouse. In order to link together the Altos, the Xerox PARC team also created **Ethernet**, which became a networking standard throughout the computer industry. Ultimately, however, Xerox failed in its attempt to market a commercial personal computer.

In 1979 Apple Computer sold 10 percent of its stock to Xerox. In return, Xerox let Steve Jobs and some Apple engineers visit Xerox PARC to learn more about its research. Jobs returned from the visit committed to building a computer with a graphical user interface. A few years later Apple released the Lisa, a $10,000 personal computer with a graphical user interface. The price tag was too high, the processor was too slow, and the Lisa was not commercially successful. However, in January 1984 Apple released the Macintosh, a faster $2,495 computer with a graphical user interface. The Macintosh was an instant hit: Apple sold 300,000 in the first year.

During the 1980s IBM, VisiCorp, and Microsoft all offered graphical user interfaces for IBM PC-compatible computers, but they could not compare in sophistication to the interface of the Apple Macintosh. Finally, in May 1990 Microsoft released Windows 3.0 for IBM PCs. Consumers eagerly bought 10 million copies of Windows, giving Microsoft a near monopoly in the graphical user interface market that it has maintained ever since.

1.4.7 Single-Computer Hypertext Systems

In 1982 Peter Brown at the University of Kent at Canterbury started a hypertext research project. He named the software Guide. Later, Office Workstations Ltd. commercialized Guide, releasing versions for both the Apple Macintosh and the IBM PC.

In 1987 Apple Computer released HyperCard, a hypertext system that enabled programmers to create “stacks” of “cards.” A card could contain text and images. The HyperCard programmer created links from one card to another with “buttons.” Buttons could be visible to the user

and labeled, or they could be transparent and associated with an image or an area of the card.

Users typically viewed one card at a time. They jumped from one card to another by using the computer's mouse to move a cursor over a button and then clicking the mouse. The best-selling computer games Myst and Riven were actually HyperCard stacks.

1.4.8 Networked Hypertext: World Wide Web

Tim Berners-Lee is the son of two mathematicians, both of whom were programmers for the Ferranti Mark 1 computer in the 1950s. From them, Berners-Lee learned that, "in principle, a person could program a computer to do most anything" [**52**, p. 3]. He also learned that it is easy to get a computer to keep information in lists or tables, but much more difficult to get it to remember arbitrary relationships.

When Berners-Lee was in high school, his father read some books about the brain; the two of them talked about how a computer might be able to make neural-like connections the way a brain does. This idea stuck with Berners-Lee, and in 1980, while working for CERN in Switzerland, he wrote a

program called Enquire that incorporated links between information. Berners-Lee was not familiar with the work of Vannevar Bush, Ted Nelson, or Doug Engelbart, but he was heading in the same direction.

In late 1989 Berners-Lee wrote a memo to a management team at CERN, proposing the development of a networked hypertext system that could be used for documentation purposes. When they didn't respond, he tried again in the spring of 1990. Again, no response. However, an intriguing new personal computer called the NeXT had just been released. Berners-Lee asked his boss if he could purchase a NeXT to check out its operating system and programming environment. His boss okayed the purchase, then puckishly suggested that maybe Berners-Lee ought to test the system's capabilities by implementing his proposed hypertext system on it [**52**].

Unlike earlier commercial hypertext systems, Berners-Lee's system allowed links between information stored on *different* computers connected by a network. Because it is built on top of the TCP/IP protocol, links can connect any two computers on the Internet, even if they have different hardware or are running different operating systems.

A **Web browser** is a program that allows a user to view Web pages and traverse hyperlinks between pages. Berners-Lee completed the first Web browser on the NeXT computer on Christmas Day 1990. He called his browser WorldWideWeb. In March 1991 he released the browser to some computer users at CERN.

In 1995 Netscape Navigator was by far the most popular Web browser. Late in that year, Microsoft made available for free to Windows users its own new Web browser, called Internet Explorer. Beginning in 1997, Microsoft integrated Internet Explorer into Windows. Everyone purchasing a Windows PC had Internet Explorer preinstalled, with its icon on their desktop. Unsurprisingly, Internet Explorer quickly began gaining market share. In 1998 the US Department of Justice sued Microsoft for abusing its dominant position in the PC market and restricting the market for competing Web browsers. In 2000 the court ruled that Microsoft's dominance of PC-based operating systems was a monopoly, and the judge ordered Microsoft to be broken up. However, the ruling was overturned on appeal in 2002. By 2003 Internet Explorer had a market share of 95% [**53**, **54**].

Today, the most popular Web browsers are Chrome, Edge, Safari, and Firefox. These browsers enable Web surfers to

retrieve text, still images, videos, songs, computer programs —in theory, anything that can be digitized. The Web has also become a convenient way for organizations to provide access to news updates and dynamically changing information.

1.4.9 Search Engines

A **search engine** is a program that accepts a list of keywords from a user, searches a database of documents, and returns those documents most closely matching the specified keywords. Today the term is most frequently used to describe programs that search databases of Web pages. Web search engines are the most powerful information retrieval devices ever invented. The precision of a search engine refers to its ability to return links to relevant documents close to the top of the list of search results. High precision is important because most users don't want to look beyond the first several results to find the Web page they want. The most popular Web search engine, Google, indexes hundreds of billions of Web pages with high precision. Google's Book Search allows users to search the full text of millions of books [55].

One of the keys to the high precision of the Google search engine is an algorithm called PageRank that helps order the

pages it returns in response to a user query. Page-Rank is based on the assumption that a good measure of the importance and quality of a Web page is how often it is referenced by other Web sites. Rather than relying solely on the presence of the search terms in a Web page to determine its relevance, PageRank counts the number and quality of links to a page from other Web sites [**56**].

1.4.10 Cloud Storage

The term **cloud storage** refers to a model of storing data remotely on servers accessed through the Internet, in contrast to storing data locally on a computer's own hard drive or other mass storage device. The cloud as a metaphor for the Internet goes back to the 1990s, if not earlier [**57**], but the word entered the popular lexicon with the introduction of easy-to-use cloud storage services, including Dropbox, Box, Google Drive, iCloud from Apple, Amazon Drive, Mega, and pCloud.

Cloud storage services allow customers to use their mobile devices, such as smart phones and laptops, to access their data from any location with an Internet connection. Cloud storage also simplifies the sharing of data files among multiple users. The availability of huge amounts of data

storage at a relatively low cost and automatic backups of data are two other important benefits of cloud storage.

1.5 Contemporary Information Technology Issues

Information technology (IT) refers to devices used in the creation, storage, manipulation, exchange, and dissemination of data, including text, sound, and images. Computers, networks, smartphones, and USB flash drives are examples of IT. The cost of IT devices continues to fall while their capabilities continue to increase. As a result, people are making greater use of IT in their everyday lives. Some of these uses create new issues that need to be resolved. Let's look at a few of the questions raised by the growth of IT.

For modern digital media, making the original copy is expensive, but making copies of the original is inexpensive. For example, entertainment companies spend vast sums producing songs, movies, and television shows, but once they have been digitized, the Internet provides a fast and free way to distribute them. In April 2015 more than a million people in the United States alone illegally downloaded the first

episode of the fifth season of *Game of Thrones*, which was leaked online a day before appearing on HBO [58]. Creators of computer software are also affected. About three-quarters of the users of Microsoft products in China do not have properly licensed software. In March 2015 Microsoft announced it would be offering free upgrades to the Windows 10 operating system to all Windows users, regardless of whether they were running genuine or illegally obtained copies of Windows [59]. What are reasonable intellectual property rights in the Information Age? Do the laws need to change? How must businesses adapt?

Cloud storage services make it convenient for a user to save photos, videos, music, and important documents, access them from multiple devices, and share them with others. However, storing data in the cloud raises reliability and security concerns. Will remotely stored data always be accessible when needed, yet remain safe from hackers?

The convenience of credit cards is undeniable, but when credit card information is stolen, it can be decidedly inconvenient for customers to determine the fraudulent charges, report them to the issuer, fill out the paperwork, and wait for the replacement card to arrive. Sometimes card information is stolen on a massive scale, affecting millions of

consumers. In November and December of 2013, hackers broke into computers at Target and stole credit card data, phone numbers, and email addresses of at least 12 million Target customers [60]. Credit card companies credit the accounts of consumers who have fraudulent charges and debit the accounts of merchants who sell goods to thieves using stolen card information. That's good for credit card holders but bad for small businesses who have no idea the cards are stolen.

The use of credit cards raises privacy concerns, too. When I use a credit card to purchase an item, the credit card company now has information about my spending habits. Who has a right to that information? If I buy a set of golf clubs with my credit card, does the credit card company have a right to sell my name, address, and phone number to other companies that may want to sell me related products?

The use of IT has changed the way that banks process loan applications. Rather than using a personal interview to decide my creditworthiness, the bank consults a national credit bureau. What are the advantages and disadvantages of this alternative approach to lending money?

Computers are now embedded in many devices on which we depend, from traffic signals to pacemakers. Software errors

have resulted in injury and even death. When bugs result in harm to humans, what should the liability be for the people or corporations that produced the software?

When employees use IT devices in their work, companies can monitor their actions closely. For example, a company can track the number of calls per minute each of its telephone operators is handling. It can document the number of keystrokes per minute of its data-entry operators. It can log all the Web sites its employees visit, and it can read the email they send and receive at work. How does such monitoring affect the workplace? Does it create an unacceptable level of stress among employees?

During the COVID-19 pandemic, many people in developed nations worked from home, thanks to IT. After the pandemic, a significant number of them did not want to return to "business as usual." What are the the advantages and disadvantages of remote work?

IT capabilities are leading to changes in the IT industry itself. Silicon Valley used to be the epicenter of the IT industry, but improvements in the speed and reliability of communication networks have led to a more decentralized landscape. Hotspots of innovation now include Seattle, Washington (Amazon, Expedia, and Microsoft); Austin, Texas (Advanced

Micro Devices, Cisco Systems, and Dell); Beijing, China (Baidu, Bytedance, Lenovo, and Xiaomi); Walldorf, Germany (SAP); and Bangalore, India (Infosys and Wipro). US-based software companies are doing more development in countries where salaries are much lower, such as India, China, and Vietnam [**9**]. Will this trend continue? How many software jobs in the United States will be lost to countries where labor is paid significantly less?

Human rights organizations have criticized Foxconn, the contract manufacturer that makes electronic devices for Apple, Amazon, Dell, and HP, for placing its Chinese employees in unsafe working conditions and forcing them to work longer than the Chinese legal maximum of 49 hours per week [**61**]. Should consumers of electronic devices boycott products that are made under unsafe or illegal conditions, or would such boycotts actually make conditions worse for workers in developing nations by depriving them of an income?

Developments in information technology have opened up unprecedented opportunities for people to share information outside the mainstream news media. Empowered individuals can lead grassroots reform movements. They can also generate and spread "fake news." Will the freewheeling

exchange of information made possible by new technologies strengthen western democracies or undermine them?

1.6 Views of Technology

In the previous section, we considered some contemporary issues that have arisen due to the adoption of information technology. How we approach these issues and others that arise is influenced by how we view the relationship between technology and society. In this section, we introduce five philosophical views of technology: instrumentalism, pragmatism, technological determinism, the cultural approach to technology, and decolonial technical design. These views apply to all technologies, not just information technologies, so let's begin by defining technology.

Technology is the application of engineering knowledge to solve practical problems. The products of technology may be tangible, such as tools and machines, or intangible, such as software.

The traditional view of technology, called **instrumentalism**, sees technological devices as instruments created by engineers to achieve ends dictated by society. Instrumentalists focus on the benefits of technology. They see technology as expanding

human capabilities, which is desirable. While it is true that a technology may be put to a bad use, that is the fault of the human users of the technology, not the creators of the technology or the technology itself, according to this view. The **neutrality thesis** holds that technology is neither good nor bad; it is the users of that technology who determine whether it will be put to good or bad use. A well-known example of this perspective is the statement, "Guns don't kill people. People kill people."

Most modern philosophers of technology do not subscribe to the view that technology is value neutral. They point out that technology is created with a goal in mind. High-quality technological creations are efficient at achieving the goals for which they were designed, and they are much less efficient at accomplishing other goals. Hence there is a connection between technologies and goals, and the moral value of the goals "rubs off" on the technologies employed to achieve them [**62**].

Like instrumentalism, **pragmatism** is another view of technology that focuses on the role of technological devices in solving practical problems. Unlike instrumentalists, however, pragmatists do not think technology is value neutral. Rather, in their view, the value of a technology is dependent on the

social context in which it is deployed. For example, urban coal-fired steam-heating plants would have been viewed favorably in the 1880s because they were a cleaner and more efficient source of heat than the alternatives available at that time. Today, the same technology would be seen as harmful because climate change is an important social concern, and coal-fired plants emit more carbon dioxide than alternative heat sources.

Technological determinism is the view that technological advancements are the most important driver of social, economic, and cultural change. According to this view, technological change is autonomous and inevitable, as expressed in the familiar saying, "You can't stop progress." Technological determinists can point to historical events supporting their view. For example, the early adoption of gunpowder in Turkey enabled the creation the Ottoman Empire, and the invention of the printing press was a catalyst for the creation of nation-states in Western Europe. Modern commentators who see the rise of AI as unstoppable are reflecting a deterministic view of technology.

Critics of technological determinism argue that the theory is too simplistic and ignores the fact that societies do have some choice regarding whether to adopt new technologies. The

cultural approach to technology holds that technology is an expression of human culture. Technology is value-laden because once adopted, it can impact society by making it easier for people to achieve some goals and more difficult for them to achieve others [**62**]. For example, as described earlier in this chapter, the adoption of the telephone facilitated long-distance communication, and the telephone also eroded traditional social hierarchies and generated new concerns about privacy.

Underlying the European colonization of the lands and people of America, Asia, and Africa was a belief system that presumed the racial inferiority of the colonized people and the inferiority of their knowledge and values. **Coloniality** refers to the situation in which these beliefs have been internalized and have persisted, even though colonialism is largely relegated to the past. Ex-colonized people believing that they are incapable of developing high quality technologies is a symptom of coloniality. Another symptom of coloniality is the view of some North Americans or Europeans that they can solve technical problems in developing nations without any help from the people who live there. Decolonial technical design is the view that a pluralistic technical design process can overcome coloniality

by including the knowledge, values, and world views of formerly colonized people [**63**].

Summary

We are living in the Information Age, an era characterized by ubiquitous computing and communication devices that have made information much easier to collect, store, retrieve, manipulate, and transmit. These devices are the culmination of centuries of technological progress.

What conclusions can we draw from our study of the development of computers, communication networks, and information storage and retrieval devices? First, revolutionary discoveries are rare. Most innovations represent simply the next step in a long staircase of evolutionary changes. Each inventor, or team of inventors, relies upon prior work. In many cases different inventors come up with the same "original" idea at the same time.

A second conclusion we can draw from these stories is that the impact of information technology on society did not begin with the personal computer and the World Wide Web. Many other inventions, including the telegraph, the telephone, the mechanical calculator, the radio, and the

television, led to significant social changes when they were adopted.

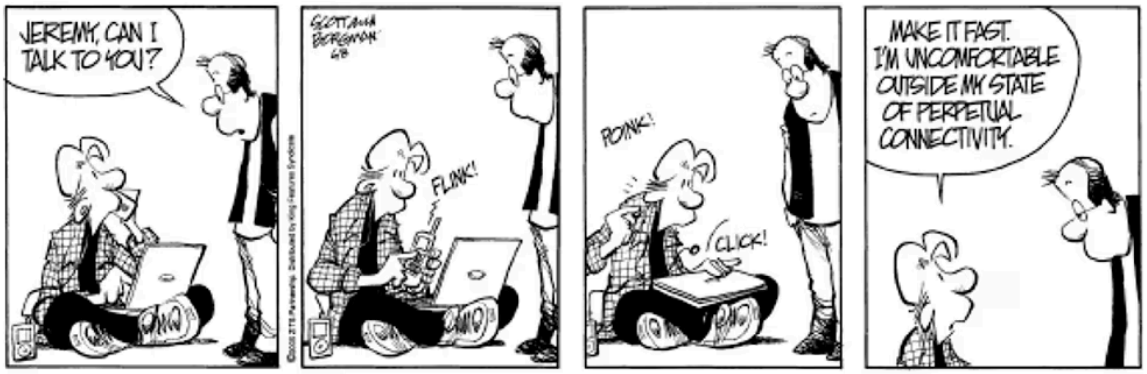
Finally, the rapid rate of technological change is causing a number of important new questions to emerge that test our values. Is it right for an AI program to produce a work of art without any compensation to the artists whose works were used to train the AI? Is it wrong for a government to keep track of every telephone call made by its citizens? Is it wrong to contribute to the development of autonomous automobiles that could put hundreds of thousands of taxicab drivers out of work?

The use of a new technology can have a significant impact on a society, but we need to remember that, as societies and as individuals, we have a great deal of control over how we choose to use a technology in order to maintain the values we hold to be fundamentally important. As Seymour Papert observed:

> **So we are entering this computer future; but what will it be like? What sort of a world will it be? There is no shortage of experts, futurists, and prophets who are ready to tell us, but they don't agree. The Utopians promise us a new millennium, a wonderful world in which the computer will solve all our problems. The**

computer critics warn us of the dehumanizing effect of too much exposure to machinery, and of disruption of employment in the workplace and the economy.

Who is right? Well, both are wrong—because they are asking the wrong question. The question is not "What will the computer do to us?" The question is "What will we make of the computer?" The point is not to predict the computer future. The point is to make it. [64]



© Zits Partnership, King Features Syndicate

Zits © 2005 Zits Partnership, Distributed by King Features Syndicate, Inc.

Further Reading, Listening, and Viewing

Adam Alter. "Why Our Screens Make Us Less Happy." *TED2017*, April 2017. 9:29. www.ted.com/talks/adam_alter_why_our_screens_make_us_les

Jim Axelrod. "Communities Fight Back Against Congestion-Causing Traffic Apps." *CBS News*, January 10, 2018. 2:09. www.cbsnews.com/news/traffic-apps-waze-traffic-nightmare-leonia-nj/.

Nicholar Carr. "Is Google Making Us Stupid?" *Atlantic*, July/August 2008.

Maciej Cegłowski. "I'm Going to Antarctica for the Penguins and to Hide from the Internet." *Wired*, March 23, 2016. www.wired.com.

Charles Duhigg and David Barboza. "In China, the Human Costs That Are Built into an iPad." *New York Times*, January 26, 2012.

"The Teenager Leading the Smartphone Liberation Movement." Interview of Logan Lane. First Person (podcast). Hosted by Lulu Garcia-Navarro. 39:41.

February 2, 2023.
https://www.nytimes.com/2023/02/02/opinion/teen-luddite- smartphones.html.
Michelle Goldberg. “Don’t Let Politics Cloud Your View of What’s Going On with Teens and Depression.” *New York Times*, February 24, 2023.
https://www.nytimes.com/2023/02/24/opinion/social-media-and-teen-depression.html.

Andrew Keen. “Opinion: Facebook Threatens to ‘Zuck Up’ the Human Race.” CNN.com, May 30, 2012.
www.cnn.com.

Erik Kruse. “On the Brink of a Networked Society.” *BOLDtalks*, April 1, 2013. 18:36.
www.youtube.com/watch?v=iazoyHS5tZ4.

Alexis C. Madigral. “The Perfect Selfishness of Mapping Apps.” CityLab (Web site), March 15, 2018.
www.citylab.com.

Robert Rosenberger. “Viewpoint: The Problem with Hands-Free Dashboard Cellphones.” *Communications of the ACM*, April 2013.

Paul Solman. “How Virtual Reality Games Can Transform Society, Prosperity.” *PBS News-Hour*, July

11, 2013. 10:27. video.pbs.org.

John D. Sutter. “Despite Horses and Buggies, Amish Aren’t Necessarily ‘Low-Tech.’” CNN.com, June 22, 2011. www.cnn.com.

Tish Harrison Warren. “We Should Be More ‘Amish’ About Technology.” *New York Times*, May 21, 2023. https://www.nytimes.com/2023/05/21/opinion/technology-teenagers-religion.html.

Carlos Watson. “Is Technology Making Us Smarter or Dumber?” *Point Taken*, June 21, 2016. 26:47. www.pbs.org/video/point-taken-technology-making-us-smarter-or-dumber-2.

Tea Uglow. “An Internet Without Screens Might Look Like This.” *TEDxSydney*, May 2015. 8:24. https://www.ted.com/talks/tom_uglow_an_internet_without_sc

Review Questions

1. Some examples of information technology, such as the alphabet and the abacus, are more than 2,000 years old. What about the present era distinguishes it as the Information Age?

2. How did the popularity of mathematical tables stimulate the development of autonomous calculating machines?

3. Compare and contrast the social conditions in the United States that stimulated the growth of the mechanical calculator market in the latter half of the nineteenth century with the social conditions that stimulated the growth of the personal computer market in the latter half of the twentieth century.

4. The Burroughs Adding Machine Company dominated the mechanical calculator market in the 1890s, and IBM dominated the electronic computer industry in the 1960s. What did these companies have in common that

led them to the number-one position in their respective markets?

5. Name three ways the development of radar in World War II stimulated advances in computing.

6. In what way did the Cold War help bring about the personal computer?

7. Can you think of a practical reason why the semaphore telegraph was adopted more rapidly on the continent of Europe than in the British Isles?

8. Compare and contrast the social impact of these three information technologies: the telegraph, the telephone, and wireless networks.

9. In what important ways did the hypertext system of Berners-Lee differ from earlier hypertext systems?

10. Give four examples from this chapter of how a social condition influenced the development of a new information technology.

11. Give four examples from this chapter of a social change caused or accelerated by the adoption of a new information technology.

12. Compare and contrast the four views of technology presented in the chapter. Which of these views most closely fits the author's presentation of the history of computing, networking, and information storage and retrieval?

Discussion Questions

13. Think about the last piece of consumer electronics you purchased. How did you first learn about it? What factors (features, price, ease of use, etc.) did you weigh before you purchased it? Which of these factors were most influential in your purchase decision? Are you still happy with your purchase?

14. Do you tend to acquire new technological devices before or after the majority of your friends? What are the advantages of being an early adopter of a new technology? What are the advantages of being a late adopter of a new technology?

15. Have you ever gone camping or had another experience where you went for at least a few days without access to a phone, radio, television, or computer? (In other words, there was no communication between you and the outside world.) What did you learn from your experience?

16. Are there any information technologies that you wish had never been adopted? If so, which ones?

17. The telephone eroded traditional social hierarchies. Has email had the same effect within colleges and universities? Do students send emails to people they would be uncomfortable talking with personally? Are these emails effective?

18. Is the cell phone changing our views about polite and impolite behavior? For example, is it polite for someone to be talking on their cell phone while ordering a drink at Starbucks?

19. Would you rather text someone than call them? Why or why not?

20. Martin Carnoy writes, "Thanks to a communications and software revolution, we are more 'connected' than ever before—by cell phone, email, and video conferencing—yet more disconnected than in the past from social interaction" [**65**]. Do you agree?

21. Was it wrong for Altair 8800 owners to use Altair BASIC on their computers without paying Micro-Soft?

22. The story of Altair BASIC highlights a clash between those who see software as something to be developed

and freely shared among computer enthusiasts and those who see software development as an entrepreneurial activity. Give some contemporary examples that illustrate these contrasting views of software.

23. More than 90 percent of personal computers run a version of the Microsoft Windows operating system. In what ways is this situation beneficial to computer users? In what ways does this situation harm computer users?

24. Angelo says, "When I'm trying to have a face-to-face conversation with someone, and that person repeatedly interrupts the conversation to answer their cell phone or exchange text messages, they are basically telling me that I'm not worth all of their attention." Do you agree with Angelo?

25. Does the widespread use of cloud computing and cloud storage by consumers represent an abandonment of the antiestablishment, "power-to-the-people" vision that fueled the growth of the personal computer industry?

26. Do you agree or disagree with the neutrality thesis?

27. Do you believe that technological progress is unstoppable?

28. How did the COVID-19 pandemic affect the development and adoption of new information technologies?

29. Predict the social changes that will take place if autonomous cars and trucks (vehicles capable of driving themselves with no human intervention) become the norm.

30. How would the widespread use of generative AI technologies such as ChatGPT and Dall-E change society?

In-Class Exercises

31. Managers of health clubs are concerned that people in locker rooms may be secretly photographed by other members carrying smartphones.

    Divide the class into groups of about four students. Each group should discuss the following proposition: "Health clubs should ban all smartphone use within their premises." After a reasonable length of time, groups should take turns sharing their conclusions with the rest of the class.

32. In the 1984 presidential election, all the major television networks used computers to predict that Republican Ronald Reagan would defeat Democrat Walter Mondale, even before the polls closed on the West Coast. When they heard this news, some Mondale supporters who had been waiting in line to vote simply went home without voting. Although the national election was already settled, the TV networks may have influenced the results of some statewide and local elections.

Divide the class into groups of about four students. Each group should discuss the pros and cons of the following proposition: “In presidential elections, the polls should close at the same time everywhere in the United States.” After a reasonable length of time, the groups should take turns sharing their conclusions with the rest of the class.

33. Read about “Star Wars Kid” and “The Bus Uncle” on Wikipedia, then have small groups discuss the following proposition: “It is wrong to post a photo or video of someone else on the Internet without their permission.”

References

[1] Linda Lacina. "Nearly 3 Billion People Around the Globe Under COVID-19 Lockdowns—Today's Coronavirus Updates." *World Economic Forum*, March 26, 2020. https://www.weforum.org/agenda/2020/03/todays-coronavirus-updates/.

[2] Erin Richards, Elinor Aspegren, and Erin Mansfield. "A Year into the Pandemic, Thousands of Students Still Can't Get Reliable WiFi for School. The Digital Divide Remains Worse than Ever." *USA Today*, February 4, 2021. www.usatoday.com/story/news/education/2021/02/04/covid-online-school-broadband-internet-laptops/3930744001/

[3] "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory." https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social- media-advisory.pdf. Accessed June 20, 2023.

[4] Ethan S. Bromberg-Martin and Okihide Hikosaka. "Midbrain Dopamine Neurons Signal Preference for

Advance Information about Upcoming Rewards." *Neuron*, 26: 119–126, July 16, 2009.

[5] Susan Weinschenk. "100 Things You Should Know About People: #8—Dopamine Makes You Addicted to Seeking Information." *What Makes Them Click: Applying Psychology to Understand How People Think, Work, and Relate* (blog), November 7, 2009. www.whatmakesthemclick.net.

[6] Christine Rosen. "Our Cell Phones, Ourselves." *New Atlantis: A Journal of Technology & Society*, Summer 6: 26–45, 2004.

[7] Howard Rheingold. "Look Who's Talking." *Wired* (7.01), 7(1): 128–131, January 1999.

[8] Alexis C. Madigral. "The Perfect Selfishness of Mapping Apps." CityLab (Web site), March 15, 2018. www.citylab.com.

[9] "The New Geography of the IT Industry." *The Economist*, 368(8333): 53–55 , July 19, 2003.

[10] "Most Nuclear Power Plants Were Built Between 1970 and 1990." Web page, U.S. Energy Information Administration, April 27, 2017.

https://www.eia.gov/todayinenergy/detail.php?id=30972.

[11] Peggy A. Kidwell and Paul E. Ceruzzi. *Landmarks in Digital Computing: A Smithsonian Pictorial History*. Smithsonian Institution Press, Washington, DC, 1994.

[12] James Cortada. *Before the Computer: IBM, NCR, Burroughs, and Remington Rand and the Industry They Created, 1865–1956*. Princeton University Press, Princeton, NJ, 2000.

[13] "A Better Day's Work at Less Cost of Time, Work, and Worry to the Man at the Desk: In Three Parts Illustrated," 3d ed. Burroughs Adding Machine Company, Detroit, MI, 1909.

[14] Sharon H. Strom. "'Machines Instead of Clerks': Technology and the Feminization of Bookkeeping, 1910–1950." In *Computer Chips and Paper Clips: Technology and Women's Employment, Volume II: Case Studies and Policy Perspectives*, edited by Heidi I. Hartmann, Robert E. Kraut, and Louise A. Tilly. National Academies Press, Washington, DC, pp. 63–97, 1987.

[15] Edwin Black. *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*. Dialog Press, Washington, DC, 2011.

[16] Joel Shurkin. *Engines of the Mind: The Evolution of the Computer from Mainframes to Microprocessors*. W.W. Norton & Company, New York, NY, 1996.

[17] Grace Murray Hopper. "Keynote Address." In *History of Programming Languages*, edited by Richard L. Wexelblat. Academic Press, New York, NY, pp. 7–20, 1981.

[18] John Backus. "The History of FORTRAN I, II, and III." In *History of Programming Languages*, edited by Richard L. Wexelblat. Academic Press, New York, NY, pp. 25–45, 1981.

[19] Jean E. Sammet. "The Early History of COBOL." In *History of Programming Languages*, edited by Richard L. Wexelblat. Academic Press, New York, NY, pp. 199–243, 1981.

[20] Thomas E. Kurtz. "Basic." In *History of Programming Languages*, edited by Richard L. Wexelblat. Academic Press, New York, NY, pp. 515–537, 1981.

[21] Robert Buderi. *The Invention That Changed the World: How a Small Group of Radar Pioneers Won the Second World War and Launched a Technological Revolution*. Simon and Schuster, New York, NY, 1996.

[22] Michael Riordan and Lillian Hoddeson. *Crystal Fire: The Birth of the Information Age*. W. W. Norton & Company, New York, NY, 1997.

[23] Frederick Seitz and Norman G. Einspruch. *Electronic Genie: The Tangled History of Silicon*. University of Illinois Press, Urbana, IL, 1998.

[24] John Markoff. *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry*. Penguin Books, New York, NY, 2005.

[25] Steve Jobs. "You've Got to Find What You Love." Commencement speech, Stanford University, June 12, 2005.

[26] Fred Turner. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. University of Chicago Press, Chicago, IL, 2006.

[27] *The People's Computer Company*, Issue 1, cover, October 1972.

[28] Paul Carroll. *Big Blues: The Unmaking of IBM*. Crown Publishers, New York, NY, 1993.

[29] Sidney H. Aronson. "Bell's Electrical Toy." In *The Social Impact of the Telephone*, edited by Ithiel de Sola Pool. MIT Press, Cambridge, MA, pp. 27–31, 1977.

[30] Carolyn Marvin. *When Old Technologies Were New: Thinking About Electric Communications in the Late Nineteenth Century*. Oxford University Press, New York, NY, 1988.

[31] "Telephone Cranks." *Western Electrician* (Chicago), p. 37, July 17, 1897.

[32] Ithiel de Sola Pool. "Introduction." In *The Social Impact of the Telephone*, edited by Ithiel de Sola Pool. MIT Press, Cambridge, MA, p. 1, 1977.

[33] Asa Briggs. "The Pleasure Telephone." In *The Social Impact of the Telephone*, edited by Ithiel de Sola Pool. MIT Press, Cambridge, MA, p. 41, 1977.

[34] Martin Campbell-Kelly and William Aspray. *Computer: A History of the Information Machine*. BasicBooks, New York, NY, 1996.

[35] James Wood. *History of International Broadcasting*. Peter Peregrinus, London, United Kingdom, p. 12, 1992.

[36] "War of the Worlds, Orson Welles, and the Invasion from Mars." Transparency (Web site). www.transparencynow.com.

[37] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. *A Brief History of the Internet, Version 3.32*, December 10, 2003. www.isoc.org/internet/history/brief.shtml.

[38] Vinton G. Cerf and Robert E. Kahn. "A Protocol for Packet Network Intercommunication." *IEEE Transactions on Communications*, COM-22(5), pp. 637–648, May 1974.

[39] Josh Fomon. "The Speedtest Global Index Shows These Countries Sped Forward for Internet Experience in 2022." *Ookla*, January 4, 2023. https://www.ookla.com/articles/global-index-internet-speed-growth-2022.

[40] "Mobile Phone Ownership." *International Telecommunication Union*. https://www.itu.int/itu-

d/reports/statistics/2022/11/24/ff22-mobile-phone-ownership/. Accessed June 29, 2023.

[41] Laurent Gloaguen. “Understanding Cloud Computing.” Spiria (blog), October 14, 2016. www.spiria.com. Accessed February 11, 2018.

[42] Martin Dodge. “An Atlas of Cyberspaces: Historical Maps of Computer Networks.” http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeog atlas/historical.html. Accessed February 11, 2018.

[43] Eric Knorr. “What Is Cloud Computing? Everything You Need to Know Now.” *InfoWorld*, July 10, 2017. www.infoworld.com.

[44] David Diringer and David R. Olson. “Greek Alphabet.” Brittanica. www.brittanica.com.

[45] Thomas Cahill. *How the Irish Saved Civilization: The Untold Story of Ireland’s Role from the Fall of Rome to the Rise of Medieval Europe*. Anchor Books, New York, NY, 1995.

[46] Elizabeth L. Eisenstein. *The Printing Press as an Agent of Change*. Volume 1. Cambridge University Press, Cambridge, England, 1979.

[47] Vannevar Bush. “As We May Think.” *Atlantic Monthly*, 176(1):101–108, August 1945.

[48] Owen Edwards. “Ted Nelson.” *Forbes ASAP*, August 25, 1997.

[49] Lauren Wedeles. “Prof. Nelson Talk Analyzes P.R.I.D.E.” *Vassar Miscellany News*, February 3, 1965.

[50] Tia O’Brien. “From the Archives: Douglas Engelbart’s Lasting Legacy, 1999.” *San Jose Mercury News*, July 3, 2013.

[51] “Internet Pioneers: Doug Engelbart.” ibiblio (Web site), www.ibiblio.org/pioneers/engelbart.html. Accessed September 23, 2013.

[52] Tim Berners-Lee. *Weaving the Web*. HarperCollins Publishers, New York, NY, 1999.

[53] “Browser Wars.” Wikipedia, https://en.wikipedia.org/wiki/Browser_wars#First_browser_war_(1995%E2%80%932001). Accessed July 25, 2023.

[54] “United States v. Microsoft Corp.” Wikipedia, https://en.wikipedia.org/wiki/United_States_v._Microsoft_Corp Accessed July 25, 2023.

[55] "How Search Organizes Information." Google (Web site). www.google.com/search/howsearchworks/crawling-indexing/. Accessed March 19, 2018.

[56] Sergey Brin and Lawrence Page. "The Anatomy of a Large-Scale Hypertextual Web Search Engine." *WWW7: Proceedings of the Seventh International Conference on World Wide Web*, 107–117, April 1998.

[57] Daniela Hernandez. "Tech Time Warp of the Week: Watch AT&T Invent Cloud Computing in 1994." *Wired*, May 23, 2014. www.wired.com.

[58] *Game of Thrones* Season 5 Infographic. *Tru Optik*, April 2015. www.truoptik.com.

[59] Bill Rigby and Paul Carsten. "Microsoft Tackles China Piracy with Free Upgrade to Windows 10." *Reuters*, March 18, 2015. www.reuters.com.

[60] Ben Elgin. "Three New Details from Target's Credit Card Breach." *Bloomberg*, March 26, 2014. www.bloomberg.com.

[61] Vindu Goel. "Foxconn Audit Finds a Workweek Still Too Long." *New York Times*, May 16, 2013.

[62] Maarten Franssen, Gert-Jan Lokhorst, and Ibo van de Poel. “Philosophy of Technology.” *The Stanford Encyclopedia of Philosophy (Spring 2023 edition)*. Edward N. Zalta & Uri Nodelman (eds.). https://plato.stanford.edu/entries/technology/.

[63] Cristiano Codeiro Cruz. “Decolonizing Philosophy of Technology: Learning from Bottom-Up and Top-Down Approaches to Decolonial Technical Design.” *Philosophy & Technology*, 24: 1847–1881, 2021.

[64] Seymour Papert. “A Critique of Technocentrism in Thinking About the School of the Future.” Technical report, MIT Media Lab, September 1990. Epistemology and Learning Memo No. 2.

[65] Martin Carnoy. *Sustaining the New Economy: Work, Family, and the Community in the Information Age*, p. x. Russell Sage Foundation/Harvard University Press, New York, NY/Cambridge, MA, 2000.

Chapter 2

Introduction to Ethics

2.1 Introduction

IMAGINE HOVERING ABOVE THE EARTH IN A SPACECRAFT ON A cloudless night. Looking down upon our planet, you see beautiful constellations of artificial light (Figure 2.1). The stars in these incandescent galaxies are our communities.

Figure 2.1

Looking down on London, England, at night from space. (Courtesy of NASA)

People choose to form communities because community living has many benefits. Communities make people more secure against external dangers, and they facilitate the exchange of goods and services. Instead of each family

assuming responsibility for all of its needs, such as food, housing, clothing, education, and health care, individuals can focus on particular activities. Specialization results in higher productivity that increases the average standard of living. In addition, communities foster the development of fulfilling personal relationships.

However, there is a price to be paid for community living. Communities prohibit certain actions and make other actions obligatory. Those who do not conform to these prohibitions and obligations can be punished. Still, the fact that almost everyone *does* live in a community is strong evidence that the advantages of community life outweigh the disadvantages.

Responsible community members take the needs and desires of other people into account when they make decisions. They recognize that virtually everybody shares the **core values** of life, happiness, and the ability to accomplish goals. People who respect only their own needs and desires are taking the selfish point of view. **The ethical point of view** is the understanding that other people and their core values are also worthy of respect [**1**].

People who take the ethical point of view may still disagree over what is the proper course of action to take in a particular situation. The facts of the matter may be

disputable, or one or both parties to the discussion may reach conclusions that do not logically follow from the facts. At other times, different value judgments arising from competing ethical theories lead people to opposite conclusions. That is why it is worthwhile to have a basic understanding of the principles of logical argumentation as well as some of the most popular ethical theories. You will find an introduction to logical argumentation in Appendix B; the remainder of this chapter focuses on presenting a variety of ethical theories, evaluating their pros and cons, and showing how to use the more viable ethical theories to solve moral problems.

2.1.1 Defining Terms

A **society** is an association of people organized under a system of rules designed to advance the good of its members over time [2]. Cooperation among individuals helps promote the common good. However, people in a society also compete with each other; for example, when deciding how to divide limited benefits among themselves. Sometimes the competition is relatively trivial, such as when many people vie for tickets to a concert. At other times the competition is much more significant, such as when two start-up companies seek dominance of an emerging market. Every society has

rules of conduct describing what people ought and ought not to do in various situations. We call these rules **morality**.

A person may simultaneously belong to multiple societies, which can lead to moral dilemmas. For example, what happens when a pacifist (according to the rules of their religion) is drafted to serve in the armed forces (according to the laws of their nation)?

Ethics is the philosophical study of morality, a rational examination into people's moral beliefs and behavior. The study of ethics is particularly important right now. Our society is changing rapidly as it incorporates the latest advances in information technology. Just think about how smartphones and social apps have changed how we spend our time and interact with others! New products and services have brought us many benefits. However, some people misuse these technologies. Here are two examples. Texting is a quick, inexpensive, and effective way of communicating, but when people choose to text while driving, they put themselves and others at risk. Social media sites promote community-building, but when people use social media to spread misinformation, they can weaken democratic institutions.

2.1.2 Rationalizations

Most of us think of ourselves as good people. In fact, if a survey of US residents is indicative, almost half of us think we are better than everyone else we know [3]! Yet if we are honest with ourselves, we must admit we sometimes do things that go against our own moral standards. When we think we can get away with it, we sometimes take advantage of the benefits that come with lying and cheating a little bit [4]. To maintain our self-images as good people, we hide from ourselves and others the true reasons for our bad deeds and generate pseudo-explanations that put them in a good light [5, 6]. A **rationalization** is a moral excuse, a justification for an immoral action.

Rationalizing is a way of "short circuiting" an ethical analysis of a situation [5]. When we rationalize, we find a reason explaining why it's okay to do something, even though it goes against our own moral sensibilities. We use this reason to give ourselves permission to plunge ahead, rather than stop and think about the situation in terms of our duties, others' rights, the action's consequences, and what a virtuous person would do.

Here are some examples of rationalizations people commonly offer for doing things that fall short of their own ethical standards [5, 7]:

- Everyone else is doing it. It's normal. Who am I to say it's wrong?
- I am taking care of my family, friends, coworkers, or company.
- It isn't my call. My boss has ordered me to do it.
- There is no point in me losing my position by refusing to do it. My boss will just bring in someone else who will do it.
- I am trying to achieve an important goal, and I can't let anything get in the way of successfully reaching it.
- I don't have the luxury of time to do a thorough analysis of this situation.
- In the long run, things will work out for the best if I do this.
- Nobody will get hurt, or at least nobody will get hurt very much.

- Yes, it will hurt them, but they are bad people, and they deserve it.
- What I'm doing isn't so bad compared to what other people are doing.
- Think of all the good things I do.

If we wish to be ethical people, we must be aware of and resist our natural inclination to act selfishly and to excuse our immoral behavior with rationalizations. Instead, we should become more committed to thoughtfully analyzing moral situations.

2.1.3 Four Scenarios

As an initiation into the study of ethics, carefully read each of the following scenarios. After reflection, come up with your own answer to each of the questions.

Scenario 1

Alexis, a gifted high-school student, wants to become a doctor. Because she comes from a family

with a low income, she plans to apply for a scholarship in order to attend college. Some of her classes require students to do extra research projects in order to get an A. Her high school has a few older PCs, but there are always long lines of students waiting to use them during the school day. After school, she usually works at a part-time job to help support her family.

One evening Alexis visits the library of a private college a few miles from her family's apartment, and she finds plenty of unused PCs connected to the Internet. She surreptitiously looks over the shoulder of another student to learn a valid login/password combination. Alexis returns to the library several times a week, and by using its PCs and printers she efficiently completes the extra research projects, graduates from high school with straight As, and gets a full-ride scholarship to attend a prestigious university.

Questions

1. Was Alexis deceitful?
2. Did Alexis treat anyone unfairly?

3. Did Alexis violate anyone's rights?
4. Who benefited from Alexis's course of action and how great were the benefits?
5. Who was harmed by Alexis's course of action and how great were the harms?
6. Would you call Alexis a good role model for other students?
7. Are there better ways Alexis could have accomplished her objective?
8. Did Alexis do the right thing?

Scenario 2

An organization dedicated to reducing spam tries to get Internet service providers (ISPs) in another country to stop the spammers by protecting their email servers. When this effort is unsuccessful, the antispam organization puts the addresses of these

ISPs on its blocklist. Many ISPs in the United States consult the blocklist and refuse to accept email from the blocklisted ISPs. This action has two results. First, the amount of spam received by the typical email user in the United States drops by 25 percent. Second, tens of thousands of innocent computer users in the blocklisted country are unable to send email to friends and business associates in the United States.

Questions

1. Did the organization do anything deceitful?
2. Was the organization unfair to anyone?
3. Did the organization violate anyone's rights?
4. Who benefited from the organization's action and how great were the benefits?
5. Who was harmed by the organization's action and how great were the harms?
6. Could the organization have achieved its goals through a better course of action?

7. Did the organization do the right thing by creating the blocklist?

Scenario 3

To address the problem of accidents caused by speeding, the East Dakota State Legislature passes a law authorizing the East Dakota State Police (EDSP) to install video cameras on all its freeway overpasses. The cameras are connected to computers that can reliably detect cars traveling more than five miles per hour above the speed limit. Sophisticated image recognition software enables the system to read license plate numbers and capture high-resolution pictures of vehicle drivers. If the picture of the driver matches the driver's license photo of one of the registered owners of the car, the system issues a speeding ticket to the driver, complete with photo evidence. The new system receives extensive media coverage, and six months

after the system is put into operation, the number of people speeding on East Dakota freeways is reduced by 90 percent.

The FBI asks the EDSP for real-time access to the information collected by the video cameras. The EDSP complies with this request. Three months later, the FBI uses this information to arrest five members of a terrorist organization.

Questions

1. Did the EDSP do anything deceitful?
2. Was the EDSP unfair to anyone?
3. Did the EDSP violate anyone's rights?
4. Who benefited from the actions of the EDSP and how great were the benefits?
5. Who was harmed by the actions of the EDSP and how great were the harms?
6. What other courses of action could the EDSP have taken to achieve its objectives?
7. Did the EDSP do the right thing by complying with the request of the FBI?

Scenario 4

You are the senior software engineer at a start-up company developing an exciting new mobile app that will allow salespeople to generate and email sales quotes and customer invoices from their smartphones. You were given stock options when you joined the company, and if it has a successful initial public offering of stock, you will be able to sell these options for at least $10 million.

Your company's sales force has led a major corporation to believe your product will be available next week. Unfortunately, at this point the software still contains quite a few bugs. The leader of the testing group has reported that all of the known bugs appear to be minor, but it will take another month of testing for his team to be

confident the product contains no catastrophic errors.

Because of the fierce competition in the mobile app industry, it is critical that your company be "first to market." To the best of your knowledge, a well-established company will release a similar product in a few weeks. If its product appears first, your start-up company will probably go out of business.

Consider at least three possible actions, and for each of them, answer the following questions.

Questions

1. What are the most likely benefits and harms that will result from this action?
2. Do you have any obligations to people who may be negatively affected by your action?
3. Does this action require you to be dishonest, deceitful, or unfair to others?

Now that you have answered the three questions for each of your possible actions, what do you think is the right action to take?

Reflect on the process you used in each scenario to come up with your answers. How did you decide if particular actions or decisions were right or wrong? Were your reasons consistent from one case to the next? If someone disagreed with you on the answer to one of these questions, how would you try to convince that person that your position makes more sense?

Ethics is the rational, systematic analysis of conduct that can cause benefit or harm to other people. Because ethics is based in reason, people are required to explain *why* they hold the opinions they do. This gives us the opportunity to compare ethical evaluations. When two people reach different conclusions, we can weigh the facts and the reasoning process behind their conclusions to determine the stronger line of thinking.

It's important to note that ethics is focused on the *voluntary, moral* choices people make because they have decided they ought to take one course of action rather than an alternative. Ethics is not concerned about involuntary choices or choices outside the moral realm.

For example, if I am ordering a new car, I may get to choose whether it is red, white, green, or blue. This choice is not in the moral realm, because it does not involve benefit or harm to other people.

Now, suppose I'm driving my new red car down a city street. A pedestrian, obscured from my view by a parked car, runs out into traffic. In an attempt to miss the pedestrian, I swerve, lose control of my car, and kill another pedestrian walking along the sidewalk. While my action caused harm to another person, this is not an example of ethical decision making, because my decision was a reflex action rather than a reasoned choice.

However, suppose I did not have full control of the car because I had been driving while intoxicated. In that case the consequences of my voluntary choice to drink alcohol before driving affected another moral being (the innocent pedestrian). Now the problem has entered the realm of ethics.

2.1.4 Overview of Ethical Theories

The formal study of ethics goes back at least 2,400 years, to the Greek philosopher Socrates. Socrates did not put any of

his philosophy in writing, but his student Plato did. In Plato's dialogue called the *Crito*, the imprisoned Socrates uses ethical reasoning to explain why he ought to face an unjust death penalty rather than take advantage of an opportunity to flee into exile with his family [8].

Since the time of Socrates and Plato, philosophers have continued to develop the field of ethics by proposing and defending many different ethical theories. In this chapter we review some of them. How do we decide if a particular theory is useful? A useful theory allows its proponents to examine moral problems, reach conclusions logically, and defend those conclusions in front of a skeptical, yet open-minded audience (Figure 2.2).

Figure 2.2

A good ethical theory should enable you to make a persuasive, logical argument to a diverse audience.

Suppose you and I are debating a moral problem in front of a nonpartisan crowd. You have concluded that a particular course of action is right, while I believe it is wrong. It is only natural for me to ask you, "Why do you think doing such-and-such is right?" If you are unable to give any logical reasons why your position is correct, you are unlikely to persuade anyone. On the other hand, if you can explain the chain of reasoning that led you to your conclusion, you will be more likely to convince the audience that your position is correct. At the very least you will help reveal where there are disputed facts or values. Therefore, we will reject proposed ethical theories that are not based on reasoning from facts or commonly accepted values.

In the following sections we consider nine ethical theories—nine frameworks for moral decision making. We present the motivation or insight underlying each theory, explain how it can be used to determine whether an action is right or wrong, and give the "case for" and the "case against" the theory. The workable theories will be those that both respect the ethical point of view and make it possible for a person to present a persuasive, logical argument to a diverse audience of skeptical, yet open-minded people.

2.2 Subjective Relativism

Ethical relativism is the theory that there are no universal moral norms of right and wrong. According to this theory, different individuals or groups of people can have completely opposite views of a moral problem, and both can be right. Two particular kinds of ethical relativism we'll discuss are subjective relativism and cultural relativism.

Subjective relativism holds that each person decides right and wrong for himself or herself. This notion is captured in the popular expression, "What's right for you may not be right for me."

2.2.1 The Case For Subjective Relativism

1. *Well-meaning and intelligent people can have totally opposite opinions about moral issues*.

   For example, consider the issue of legalized abortion in the United States. There are a significant number of

rational people on each side of the issue. Subjective relativists would contend that the reason people cannot reach the same conclusion is that morality is not like gravity; it is not something "out there" that rational people can discover and try to understand. Instead, each of us creates his or her own morality.

2. *Ethical debates are disagreeable and pointless*.

   Going back to the example of abortion, the debate in the United States has been going on for more than 50 years. An agreement about whether abortion is right or wrong may never be reached. Nobody is all-knowing. When faced with a difficult moral problem, who is to say which side is correct? If morality is relative, we do not have to try to reconcile opposing views. Both sides are right.

2.2.2 The Case Against Subjective Relativism

1. *With subjective relativism the line between doing what you think is right and doing what you want to do is not sharply drawn*.

As pointed out earlier in this chapter, people are good at rationalizing their bad behavior. Subjective relativism provides an easy excuse for someone whose conduct is being questioned. When pressed to explain a decision or action, a subjective relativist can reply, "Who are *you* to tell *me* what I should and should not do?" If morality means doing whatever you want to do, it doesn't mean much, if it means anything at all. Put another way, you can't do ethics without values.

2. *By allowing people to decide right and wrong for themselves, subjective relativism makes no moral distinction between the actions of different people*.

   The fact is that some people have caused millions to suffer, while others have led lives of great service to humanity. Suppose both Adolf Hitler and Mahatma Gandhi spent their entire lives doing what they thought was the right thing to do. Do you want to give both of them credit for living good lives?

   A modification of the original formulation of subjective relativism might be, "I can decide what's right for me, as long as my actions don't hurt anybody else." That solves the problem of Adolf Hitler versus Mahatma Gandhi. However, as soon as you introduce the idea

that you shouldn't harm others, you must come to an agreement with others about what it means to harm someone. At this point the process is no longer subjective or completely up to the individual. In other words, a statement of the form, "I can decide what's right for me, as long as my actions don't hurt anyone else," is a statement expressing a universal norm, which is inconsistent with subjective relativism.

3. *Subjective relativism and tolerance are two different things*.

   Some people may be attracted to ethical relativism because they believe in tolerance. There is a lot to be said for tolerance. It allows individuals in a pluralistic society like the United States to live in harmony. However, tolerance is not the same thing as subjective relativism. Subjective relativism holds that individuals decide for themselves what is right and what is wrong. If you are a tolerant person, is it okay with you if some people decide they want to be intolerant? What if some people decide that they will only deal fairly with people of their own racial group? You can't say that racial bigotry is wrong without undermining the foundation of subjective relativism, because any statement of the form, "People ought to be tolerant," is an example of a

universal moral **norm**, or rule. Relativism is based on the idea that there are *no* universal moral norms, so a blanket statement about the need for tolerance is incompatible with subjective relativism.

4. *We should not give legitimacy to an ethical theory that allows people to make decisions based on something other than reason.*

   If individuals decide for themselves what is right and what is wrong, they can reach their conclusions by any means they see fit. They may choose to base their decisions on something other than logic and reason, such as the rolling of dice or the turning of tarot cards. This path is contrary to using logic and reason.

If your goal is to persuade others that your solutions to actual moral problems are correct, adopting subjective relativism is self-defeating because it is based on the idea that people decide for themselves what is right and what is wrong. According to subjective relativism, nobody's conclusions are any more valid that anyone else's, no matter how these conclusions are drawn. Therefore, we reject subjective relativism as a workable ethical theory.

2.3 Cultural Relativism

If subjective relativism is unworkable, what about different views of right and wrong held by different societies at the same point in time, or those held by the same society at different points in time?

In the modern era, anthropologists have collected evidence of societies with moral codes markedly different from each other. William Graham Sumner described the evolution of "folkways," which he argues eventually become institutionalized into the moral guidelines of a society:

> **The first task of life is to live. . . . The struggle to maintain existence was not carried on individually but in groups. Each profited by the other's experience; hence there was concurrence towards that which proved to be the most expedient. All at last adopted the same way for the same purpose; hence the ways turned into customs and became mass phenomena. Instincts were learned in connection with them. In this way folkways arise. The young learn by tradition, imitation, and authority. The folkways, at a time, provide for all the needs of life then and there. They are**

> **uniform, universal in the group, imperative, and invariable. As time goes on, the folkways become more and more arbitrary, positive, and imperative. If asked why they act in a certain way in certain cases, primitive people always answer that it is because they and their ancestors always have done so. . . . The morality of a group at a time is the sum of the taboos and prescriptions in the folkways by which right conduct is defined. . . . "Good" mores are those which are well adapted to the situation. "Bad" mores are those which are not so well adapted.** [9]

Cultural relativism is the ethical theory that the meaning of "right" and "wrong" rests with a society's actual moral guidelines. These guidelines vary from place to place and from time to time.

2.3.1 The Case For Cultural Relativism

1. *Different social contexts demand different moral guidelines*.

   It's unrealistic to assume that the same set of moral guidelines can be expected to work for all human societies in every part of the world for all ages. Just think about how our relationship with our environment

has changed. For nearly all of the past 10,000 years, human beings have spent most of their time trying to produce enough food to survive. Thanks to science and technology, the human population of the Earth has increased exponentially in the past century. The struggle for survival has shifted away from people to the rest of Nature. Overpopulation has created a host of environmental problems, such as the extinction of many species, the destruction of fisheries in the world's oceans, and the accumulation of greenhouse gases. People must change their ideas about what is acceptable conduct and what is not, or they will destroy the planet.

2. *It is arrogant for one society to judge another.*

   Anthropologists have documented many important differences among societies with respect to what they consider proper and improper moral conduct. We may have more technology than people in other societies, but we are no more intelligent than they are. It is arrogant for a person living in twenty-first-century Italy to judge the actions of another person who lived in the Inca Empire in the fifteenth century.

2.3.2 The Case Against Cultural Relativism

1. *Just because two societies do have different views about right and wrong doesn't imply that they ought to have different views.*

   Perhaps one society has good guidelines and another has bad guidelines. Perhaps neither society has good guidelines.

   Suppose two societies are suffering from a severe drought. The first society constructs an aqueduct to carry water to the affected cities. The second society makes human sacrifices to appease the rain god. Are both "solutions" equally acceptable? No, they are not. Yet, if we accept cultural relativism, we cannot speak out against this wrongdoing, because no person in one society can make any statements about the morality of another society.

2. *Cultural relativism does not explain how an individual determines the moral guidelines of a particular society.*

   Suppose I am new to a society and I understand I am supposed to abide by its moral guidelines. How do I

determine what those guidelines are?

One approach would be to poll other people, but this begs the question. Here's why. Suppose I ask other people whether the society considers a particular action to be morally acceptable. I'm not interested in knowing whether they feel personally that the action is right or wrong. I want them to tell me whether the society as a whole thinks the action is moral. That puts the people I poll in the same position I'm in—trying to determine the moral guidelines of a society. How are they to know whether the action is right or wrong?

Perhaps the guidelines are summarized in the society's laws, but laws take time to enact. Hence the legal code reflects at best the moral guidelines of the same society at some point in the past, but that's not the same society I am living in today, because the morals of any society change over time. That leads us to our next objection.

3. *Cultural relativism does not explain how to determine right from wrong when there are no cultural norms.*

   Sometimes different groups within a society disagree about whether a particular action is right or wrong. This situation often occurs when a new technology

emerges. For example, the Internet has made possible massive exchanges of digitized information. Millions of people in the United States seem to think sharing copyrighted music is okay, but other groups insist this activity is nothing more than stealing. Who is correct?

4. *Cultural relativism does not do a good job of characterizing actions when moral guidelines evolve.*

   Until the 1960s many southern US states had segregated universities. Today these universities are integrated. This cultural shift was accelerated by the actions of a few brave Black students who challenged the status quo and enrolled in universities that had been the exclusive preserve of white students. At the time these students were doing what they "ought not" to have done; they were doing something wrong according to the dominant culture of those states at that time. By today's standards they did nothing wrong, and many people view them as heroic figures. Doesn't it make more sense to believe that their actions were the right thing to do all along?

5. *Cultural relativism provides no framework for reconciliation between cultures in conflict.*

Think about the culture of the Palestinians who have been crowded into refugee camps in the Gaza Strip for more than 60 years. Some of these people are completely committed to an armed struggle against Israel. Meanwhile, some people in Israel believe the Jewish state ought to be larger and are completely committed to the expansion of settlements into the Gaza Strip. The values of each society lead to actions that harm the other, yet cultural relativism says each society's moral guidelines are right. Cultural relativism provides no way out—no way for the two sides to find common ground.

6. *The existence of many acceptable cultural practices does not imply that any cultural practice would be acceptable.*

   Judging many options to be acceptable and then reaching the conclusion that any option is acceptable is called the **many/any fallacy**. To illustrate this fallacy, consider documentation styles for computer programs. There are many good ways to add comments to a program; that does not mean that any commenting style is good.

It is false that all possible cultural practices have equal legitimacy. Certain practices must be forbidden and others must be mandated if a society is to survive [**1**]. This observation leads us directly to our next point.

7. *Societies do, in fact, share certain core values*.

   While a superficial observation of the cultural practices of different societies may lead you to believe they are quite different, a closer examination often reveals similar values underlying these practices. James Rachels argues that all societies, in order to maintain their existence, must have a set of core values [**10**]. For example, newborn babies are helpless. A society must care for its infants if it wishes to continue. Hence a core value of every society is that babies must be cared for. Communities rely upon people being able to believe each other. Hence telling the truth is another core value. Finally, in order to live together, people must not constantly be on guard against attack from their community members. For this reason a prohibition against murder is a core value of any society.

   The existence of common values among all societies is a powerful response to the contention that different social contexts demand different moral guidelines, which is at

the heart of the argument in favor of cultural relativism. Because societies do share certain core values, there is reason to believe we could use these values as a starting point in the creation of a universal ethical theory that would not have the deficiencies of cultural relativism.

8. *Cultural relativism is only indirectly based on reason.*

   As Sumner observed, many moral guidelines are a result of tradition. Traditions develop because they meet a need, but once a tradition has been established, people behave in a certain way because it's what they're supposed to do, not because they understand the rationality deeply embedded within the tradition.

Cultural relativism has significant weaknesses as a tool for ethical persuasion. According to cultural relativism, the ethical evaluation of a moral problem made by a person in one society may be meaningless when applied to the same moral problem in another society. Cultural relativism suggests there are no universal moral guidelines. It gives tradition more weight in ethical evaluations than facts and reason. For these reasons, cultural relativism is not a powerful tool for constructing ethical evaluations persuasive to a diverse audience, and we consider it no further.

2.4 Divine Command Theory

The three great religious traditions that arose in the Middle East—Judaism, Christianity, and Islam—teach that a single God is the creator of the universe and that human beings are part of God's creation. Each of these religions has sacred writings containing God's revelation.

Jews, Christians, and Muslims all believe that God inspired the Torah. Here is a selection of verses from Chapter 19 of the third book of the Torah, called Vayikra or Leviticus:

> **You shall each revere his mother and his father, and keep My sabbaths. When you reap the harvest of your land, you shall not reap all the way to the edges of your field, or gather the gleanings of your harvest. You shall not pick your vineyard bare, or gather the fallen fruit of your vineyard; you shall leave them for the poor and the stranger. You shall not steal; you shall not deal deceitfully or falsely with one another. You shall not swear falsely by My name. You shall not defraud your neighbor. You shall not commit robbery. The wages of a laborer shall not remain with you until morning. You shall not insult the deaf, or place a stumbling block**

> **before the blind. You shall not take vengeance or bear a grudge against your kinsfolk. Love your neighbor as yourself. [11]**

The **divine command theory** is based on the idea that good actions are those aligned with the will of God and bad actions are those contrary to the will of God. Since the holy books contain God's directions, we can use the holy books as moral decision-making guides. God says we should revere our mothers and fathers, so revering our parents is good. God says do not lie or steal, so lying and stealing are bad (Figure 2.3).

Figure 2.3

The divine command theory of ethics is based on two premises: good actions are those actions aligned with the will of God, and God's will has been revealed to us.

It is important to note that the divine command theory is subscribed to by some, but not all, Jews, Christians, and Muslims. Fundamentalists are more likely to consider holy books authentic and authoritative. Most sects within these religious traditions augment holy books with other sources when developing their moral codes.

2.4.1 The Case For the Divine Command Theory

1. *We owe obedience to our Creator*.

   God is the creator of the universe. God created each one of us. We are dependent upon God for our lives. For this reason, we are obligated to follow God's rules.

2. *God is all-good and all-knowing*.

   God loves us and wants the best for us. God is omniscient; we are not. Because God knows better than we do what we must do to be happy, we should align ourselves with the will of God.

3. *God is the ultimate authority*.

Since most people are religious, they are more likely to submit to God's law than to a law made by people. Our goal is to create a society where everyone obeys the moral laws. Therefore, our moral laws should be based on God's directions to us.

2.4.2 The Case Against the Divine Command Theory

1. *There are many holy books, and some of their teachings disagree with each other.*

   There is no single holy book that is recognized by people of all faiths, and it is unrealistic to assume everyone in a society will adopt the same religion. Even among Christians there are different versions of the Bible. The Catholic Bible has six books not found in the Protestant Bible. Some Protestant denominations rely upon the King James version, but others use more modern translations. Every translation has significant differences. Even when people read the same translation, they often interpret the same verse in different ways.

2. *It is unrealistic to assume a multicultural society will adopt a religion-based morality*.

   An obvious example is the United States. In the past two centuries, immigrants representing virtually every race, creed, and culture have made it their home. Some Americans are atheists. When a society is made up of people with different religious beliefs, the society's moral guidelines should emerge from a secular authority, not a religious authority.

3. *Some moral problems are not addressed directly in scripture*.

   For example, there are no verses in the Bible mentioning the Internet. When we discuss moral problems arising from information technology, a proponent of the divine command theory must resort to analogy. At this point the conclusion is based not simply on what appears in the sacred text but also on the insight of the person who invented the analogy. The holy book alone is not sufficient to solve the moral problem.

4. *The divine command theory is based on obedience, not reason*.

If good means "willed by God," and if religious texts contain everything we need to know about what God wills, then there is no room left for collecting and analyzing facts. Hence the divine command theory is not based on reaching sound conclusions from premises through logical reasoning. There is no need for a person to question a commandment. The instruction is right because it's commanded by God, period.

Consider the story of Abraham in the book of Genesis. God commands Abraham to take his only son, Isaac, up on a mountain, kill him, and make of him a burnt offering. Abraham obeys God's command and is ready to kill Isaac with his knife when an angel calls down and tells him not to harm the boy. Because he does not withhold his only son from God, God blesses Abraham [**12**]. However, earlier in Genesis God condemns Cain for killing Abel [**13**]. How, then, can Abraham's sacrifice of Isaac be considered good? To devout readers, the logic of God's command is irrelevant to this story. Abraham is a good person, a heroic model of faith, because he demonstrated his obedience to the will of God.

In the divine command theory, moral guidelines are not the result of a logical progression from a set of underlying principles, and this is a significant problem. While you may choose to live your life so that your actions are aligned with God's will, the divine command theory often fails to produce arguments that can persuade skeptical listeners who have different religious beliefs or no religious beliefs at all. That is why we do not consider divine command theory a workable theory for the purposes of this book.

2.5 Ethical Egoism

In sharp contrast to the divine command theory, which promotes a concern for others with scriptural injunctions such as "Love your neighbor as yourself," ethical egoism is the philosophy that each person should focus exclusively on their self-interest. In other words, according to ethical egoism, the morally right action for a person to take in a particular situation is the action that will provide that person with the maximum long-term benefit.

This idea may sound familiar to you if you have read *The Fountainhead* or *Atlas Shrugged*. The author of these novels, Ayn Rand, espoused a philosophy akin to ethical egoism (although you should not view this section's description of ethical egoism as a summary of her thinking). Rand's moral philosophy "holds man's life as the *standard* of value—and *his own life* as the ethical *purpose* of every individual man" [**14**, p. 27]. With respect to human relationships, she wrote, "The principle of *trade* is the only rational ethical principle for all human relationships, personal and social, private and public, spiritual and material" [**14**, p. 34].

Ethical egoism does not prohibit acting to help someone else, but assisting another is the right thing to do if and only if it is in the helper's own long-term best interest. For example, suppose I depend upon a friend to give me a ride to work every day. If my friend's car breaks down and she doesn't have $100 to fix it, I ought to loan her the money. Although I'm out $100 until she pays me back, I'm better off giving her the loan because I'm still able to travel to work and make money. If I don't lend her the money, I'll lose my income. Lending $100 to my friend is the right thing to do because it provides me the maximum overall benefit [**15**].

2.5.1 The Case For Ethical Egoism

1. *Ethical egoism is a practical moral philosophy.*

   We are naturally inclined to do what's best for ourselves because each of us has only one life to live, and we want to make the best of it. Unlike other moral codes that ask us to sacrifice our own well-being for the good of other people, ethical egoism recognizes that we should focus on our own well-being.

2. *It's better to let other people take care of themselves.*

   We can't know for sure what is good for someone else. All too often, a "good deed" backfires and actually does more harm than good. Even when people appreciate something done on their behalf, it's not healthy. Dependence upon the charity of others leads to a loss of self-esteem. In contrast, people who accomplish things through their own efforts have higher self-esteem and are able to interact with other successful people as equals.

3. *The community can benefit when individuals put their well-being first.*

   When individuals act in their own self-interest, they often benefit not only themselves but others as well. For example, successful entrepreneurs may make a lot of money for themselves, but they also create jobs that strengthen the economy.

4. *Other moral principles are rooted in the principle of self-interest.*

   Ethical egoism is a rational philosophy. Any rational person will figure out that it doesn't make sense to go around breaking promises, because eventually people

will realize that the promise breaker cannot be trusted, and they will refuse to cooperate with that person. Therefore, it's not in a person's long-term self-interest to break promises. Likewise, it's a bad idea to lie to other people or cheat other people because the long-term consequences of lying and cheating are detrimental to the person doing these things. For this reason, it can be seen that other well-known moral principles are actually rooted in the principle of self-interest.

2.5.2 The Case Against Ethical Egoism

1. *An easy moral philosophy may not be the best moral philosophy*.

   The fact that it may be easier to live by a particular moral philosophy is no proof that it is the best moral philosophy to live by. Besides, the statement that ethical egoism aligns with our natural inclination to do what's best for ourselves ignores the fact that our natural inclinations often do not align with our own best interests. For example, some students find it difficult to pass up short-term pleasures (such as partying) in order to achieve goals that will most likely result in long-term

benefits (such as passing the classes needed to earn a college degree).

2. *We do, in fact, know a lot about what is good for someone else*.

   As we noted at the beginning of the chapter, practically everyone shares the "core values" of life, happiness, and the ability to accomplish goals. It's not that hard to figure out what would help another. The question is, how are we going to respond to that person's need? Charity usually doesn't lead to dependence; rather, it gives someone the opportunity to become more independent. Consider, for example, how a scholarship can provide a promising high-school student from a poor family with a path to a university degree, a well-paying job, and economic self-sufficiency.

3. *A self-interested focus can lead to blatantly immoral behavior*.

   Here is a true story related by James Rachels [**16**]. An affluent doctor in a small Southern town in the 1970s was visited by an African American woman who had a very low income from a variety of low-paying jobs. The doctor quickly determined that the woman was suffering from malnutrition. He knew that she was paid

very little money to support herself or her children. After spending no more than five minutes with her, and doing nothing for her, the doctor told her the charge would be $25. The woman had only $12 to her name, so the doctor took the $12 as payment, leaving the woman with no money to buy food. There were no negative consequences to the doctor as a result of his action. According to the theory of ethical egoism, the doctor did the right thing: he was only supposed to take his own interest into account, and receiving $12 from the woman was to his advantage. This answer, however, is incorrect; what the doctor did was morally reprehensible. The first duty of a physician is to do no harm to the patient. By taking the malnourished woman's last $12, the doctor made her condition worse by pocketing money that she could have used for food.

4. *Other moral principles are superior to the principle of self-interest.*

   Suppose you have the opportunity to save a drowning person at the cost of getting one of your shirtsleeves wet [**15**]. According to the theory of ethical egoism, saving a life is the right thing to do if and only if that action will provide you with the maximum benefit. Possible benefits from saving a drowning person include earning

that person's undying gratitude and gaining favorable publicity. But isn't this a backward and degrading way of evaluating the action? Doesn't it make a lot more sense to consider the action in light of the value of a human life? If you have the opportunity to save a human life with no significant negative consequences to yourself, you should do it, even if your action is not rewarded. This example illustrates that the principle of preserving life is superior to the principle of self-interest.

5. *People who take the good of others into account live happier lives*.

   In the Framingham Heart Study, which followed 5,000 individuals over a 20-year period, scientists discovered that happiness spreads through close relationships with family members, friends, and neighbors [**17**]. In order to create and maintain close relationships with other people, it is necessary to consider what is good for them.

Ethical egoism does not respect the ethical point of view. In other words, it does not recognize that in order to reap the benefits of living in a community, individuals must consider

the good of other community members. For this reason we reject ethical egoism as a workable ethical theory.

2.6 Kantianism

Kantianism is the name given to the ethical theory of the German philosopher Immanuel Kant (1724–1804). Kant spent his entire life in or near Königsberg in East Prussia, where he was a professor at the university. Kant believed that people's actions ought to be guided by moral laws, and that these moral laws were universal. He held that in order to apply to all rational beings, any supreme principle of morality must itself be based on reason. While many of the moral laws Kant describes can also be found in the Bible, Kant's methodology allows these laws to be derived through a reasoning process. A Kantian is able to go beyond simply stating that an action is right or wrong by citing chapter and verse; a Kantian can explain *why* it is right or wrong.

2.6.1 Good Will and the Categorical Imperative

Kant begins his inquiry by asking, "What is always good without qualification?" Many things, such as intelligence and courage, can be good, but they can also be used in a way that is harmful. For example, a group of gangsters may use

intelligence and courage to rob a bank. Kant's conclusion is that the only thing in the world that can be called good without qualification is a good will. People with good will often accomplish good deeds, but producing beneficial outcomes is not what makes a good will good. A good will is good in and of itself. Even if a person's best efforts at doing good should fall short and cause harm, the good will behind the efforts is still good. Since a good will is the only thing that is universally good, the proper function of reason is to cultivate a will that is good in itself.

Most of us have probably had many experiences when we've been torn between what we want to do and what we ought to do. According to Kant, what we want to do is of no importance. Our focus should be on what we ought to do. Our sense of "ought to" is called **dutifulness** [18]. A dutiful person feels compelled to act in a certain way out of respect for some moral rule. Our will, then, should be grounded in a conception of moral rules. The moral value of an action depends upon the underlying moral rule. It is critical, therefore, that we be able to determine if our actions are grounded in an appropriate moral rule.

For Kant, an **imperative** is a way in which reason commands the will. There are two kinds of imperatives: hypothetical and

categorical. A **hypothetical imperative** is a conditional rule of the form, “If you want X then do Y” [**19**]. It explains the means you should take to achieve a particular end. An example of a hypothetical imperative would be, “If you want to lose weight then eat less.” A **categorical imperative** is an unconditional rule: a rule that always applies, regardless of the circumstances. For Kant, only a categorical imperative can be a moral imperative.

What is the Categorical Imperative, the rule that all humans should obey unconditionally, regardless of their particular circumstances and goals? Kant proposes several formulations of the Categorical Imperative, which he believes communicate the same concept in different ways. We will cover the first two formulations. Here is the first.

Categorical Imperative (First Formulation)

Act only from moral rules that you can at the same time will to be universal moral laws.

In other words, you should act only on moral rules that you can imagine everyone else following without deriving a logical contradiction [**19**].

To illustrate the Categorical Imperative, Kant poses the problem of an individual in a difficult situation who must decide if he will make a promise with the intention of later breaking it. The translation of this moral rule could be as follows: “A person may make a false promise when that is the only way to escape a difficult situation.”

To evaluate this moral rule, we universalize it. What would happen if everybody in extreme circumstances made false promises? If that were the case, nobody would believe promises, and it would be impossible for our individual in distress to make a promise that anyone believed. The moral rule self-destructs when we try to make it a universal law.

Therefore, it is wrong for a person in distress to make a promise with the intention of breaking it.

It is important to see that Kant is *not* arguing that the harmful consequences of everybody breaking promises is why we cannot imagine turning our hypothetical moral rule into a universal law. Rather, Kant is saying that simply willing that our moral rule become a universal law produces a logical contradiction.

Let's see how. Suppose I am the person who can escape from a difficult situation by making a promise I intend to break later on. On the one hand, it is my will that I be able to make a promise that is believed. After all, that's what promises are for. If my promise isn't believed, I won't be able to get out of the difficult situation I am in. But when I universalize the moral rule, I am willing that everybody be able to break promises. If that were a reality, then promises would not be believable, which means there would be no such thing as a promise [20]. If there were no such thing as a promise, I would not be able to make a promise to get myself out of a difficult situation. Trying to universalize our proposed moral rule leads to a contradiction.

Here's another way to see why the proposed moral rule cannot be made a universal moral law. In order for my false

promise to be believed, I want everyone *except* myself to be truthful all the time. In other words, I want to privilege my own needs and desires over those of everyone else [**19**]. Because there is a contradiction between what I wish to do and how I expect others in a similar situation to act, I know that what I am considering doing is wrong.

If you are wondering whether or not it is morally acceptable under Kantianism to do something to someone else, mentally reverse roles. What would you think if that person did the same thing to you? If you cannot wish to be treated that way by another, you have evidence that the action you are contemplating privileges your own needs and desires and violates the Categorical Imperative.

Kant also presents a second formulation of the Categorical Imperative that many people find easier to work with when doing ethical analyses.

Categorical Imperative (Second Formulation)

> Act so that you always treat both yourself and other people as ends in themselves, and never only as a means to an end.

To use popular terminology, the second formulation of the Categorical Imperative says it is wrong for one person to "use" another (Figure 2.4). Instead, every interaction with other people must give them the dignity and respect they deserve as autonomous, rational beings.

Figure 2.4

The second formulation of the Categorical Imperative states that it is wrong for one person to use himself or another person solely as a means to an end.

Here is an example that illustrates how we can apply the second formulation. Suppose I manage a semiconductor

fabrication plant for a large corporation. The plant manufactures integrated circuits on 8-inch wafers. I know that in one year the corporation is going to shut down the plant and move all of its production to other sites capable of producing 12-inch wafers. In the meantime, I need new employees to work in the clean room. Many of the best applicants are from out of state. I am afraid that if they knew the plant was going to shut down next year, they would not want to go through the hassle and expense of moving to this area. If that happens, I'll have to hire less qualified local workers. Should I disclose this information to the job applicants?

According to the second formulation of the Categorical Imperative, I have an obligation to inform the applicants, since I know this information is likely to influence their decision. If I deny them this information, I am treating them as a means to an end (a way to get wafers produced), not as ends in themselves (rational beings).

2.6.2 Evaluating a Scenario Using Kantianism

Scenario

Rosa is the sole financial provider for her family. She is working hard to complete her college education while caring for her daughter. If she can pass both courses this semester, she will graduate. She knows her child will benefit if she can spend more time at home.

One of her required classes is modern European history. In addition to the midterm and final examinations, the professor assigns four lengthy reports, which is far more than the usual amount of work required for a single class. Students must submit all four reports in order to pass the class.

Rosa earns an A on each of her first three reports. At the end of the term, she is required to put in a lot of overtime where she works. She simply does not have time to research and write the final report. Rosa uses the Web to identify a company that sells term papers. She purchases a report from the company and submits it as her own work.

Was Rosa's action morally justifiable?

Analysis

Many times it is easier to use the second formulation of the Categorical Imperative to analyze a moral problem from a Kantian point of view, so that's where we begin. By submitting another person's work as her own, Rosa treated her professor as a means to an end. She deceived her professor with the goal of getting credit for someone else's work. It was wrong for Rosa to treat the professor as a grade-giving machine rather than a rational agent with whom she could have communicated her unusual circumstances.

We can also look at this problem using the first formulation of the Categorical Imperative. Rosa wants to be able to get credit for turning in a report she has purchased. A proposed moral rule might be, "I may claim academic credit for a report written by someone else." However, if everyone followed this rule, reports would cease to be credible indicators of the students' knowledge, and professors would not give academic credit for reports. Her proposed

moral rule is self-defeating. Therefore, it is wrong for Rosa to purchase a report and turn it in as her own work.

Commentary

Note that the Kantian analysis of the moral problem focuses on the will behind the action. It asks the question, "What was Rosa trying to do when she submitted under her own name a term paper written by someone else?" The analysis ignores extenuating circumstances that non-Kantians may cite to justify her action.

2.6.3 The Case For Kantianism

1. *It treats all persons as moral equals*.

   A popular belief is that "all people are created equal." Because it holds that people in similar situations should be treated in similar ways, Kantianism provides an ethical framework to combat discrimination.

2. *It gives all persons moral worth by considering them as rational, autonomous beings*.

   Every human being has an inherent dignity and deserves respect [**19**]. That is why, according to Kant, other persons should always be treated as ends in themselves, not merely as the means to an end. This perspective aligns with the commonly held view that it is wrong for one person to manipulate another.

3. *Everyone is held to the same standard*.

   According to Kantianism, it is wrong for you to grant yourself an exception to a principle you expect everyone else to abide by. For example, it would be wrong to break a legal contract and also desire that everyone else in a similar circumstance would honor the contract. This basic principle of justice is a natural corollary of Kant's view that all persons are moral equals, and it is reflected in the proverb, "What's good for the goose is good for the gander."

4. *Kantianism produces universal moral guidelines*.

   Kantianism aligns with the intuition of many people that the same morality ought to apply to all people for all of history. These guidelines allow us to make clear

moral judgments. For example, one such judgment might be the following: “Sacrificing living human beings to appease the gods is wrong.” It is wrong in Europe in the twenty-first century, and it was wrong in South America in the fifteenth century.

2.6.4 The Case Against Kantianism

1. *Sometimes no single rule fully characterizes an action.*

   Kant holds that every action is motivated from a rule. The appropriate rule depends upon how we characterize the action. Once we know the rule, we can test its value using the Categorical Imperative. What happens when no single rule fully explains the situation? Suppose I’m considering stealing food from a grocery store to feed my starving children [15]. How should I characterize this action? Am I stealing? Am I caring for my children? Am I trying to save the lives of innocent people? Until I characterize my action, I cannot determine the rule and test it against the Categorical Imperative. Yet no single one of these ways of characterizing the action seems to capture the ethical problem in its fullness.

2. *Sometimes there is no way to resolve a conflict between rules.*

   One way to address the previous problem is to allow multiple rules to be relevant to a particular action. In the previous example, we might say that the relevant rules are (1) you should not steal and (2) you should try to save the lives of innocent persons. Now the question becomes, if we have a conflict between two rules, which one should we follow?

   Kant distinguished between **perfect duties**, duties we are obliged to fulfill in every instance, and **imperfect duties**, duties we are obliged to fulfill in general but not in every instance. For example, you have a perfect duty to tell the truth. That means you must always tell the truth without exception. On the other hand, you have an imperfect duty to develop your talents. If you happen to have a talent for music, you ought to find a way to develop it, but you do not have to take up every instrument in the orchestra.

   If we have a conflict between a perfect duty and an imperfect duty, the perfect duty must prevail. Returning to our example, we have a perfect duty not to steal. In contrast, we have only an imperfect duty to help others.

Therefore, according to Kant, it is wrong to steal bread to feed my starving children.

In this case we were fortunate because the conflict was between a perfect duty and an imperfect duty. (Whether the children are fortunate is debatable.) In those cases where there is a conflict between perfect duties, Kantianism does not provide us a way to choose between them.

3. *Kantianism allows no exceptions to perfect duties*.

Common sense tells us that sometimes we ought to "bend" the rules a bit if we want to get along with other people. For example, suppose someone's mother asks them if they like her new haircut, and they think it is the ugliest haircut they have ever seen. What should they say? Common sense dictates that there is no point in being critical. The mother can't get her hair uncut, no matter what anyone says. She expects a compliment, and if she doesn't get one, she will be angry and hurt. There just seems to be no downside to lying. Yet a Kantian would argue that lying is always wrong because we have a perfect duty to tell the truth. Any ethical theory so unbending is not going to be useful for solving "real-world" problems.

While these objections point out weaknesses with Kantianism, the theory does support moral decision making based on logical reasoning from facts and commonly held values. It is culture-neutral and treats all humans as equals. Hence it meets our criteria for a workable ethical theory, and we will use it as a way of evaluating moral problems in the rest of the book.

2.7 Act Utilitarianism

The English philosophers Jeremy Bentham (1748–1832) and John Stuart Mill (1806–1873) proposed a theory that is in sharp contrast to Kantianism. According to Bentham and Mill, an action is good if its benefits exceed its harms, and an action is bad if its harms exceed its benefits. Their ethical theory, called **utilitarianism**, is based upon the principle of utility, also called the Greatest Happiness Principle.

2.7.1 Principle of Utility

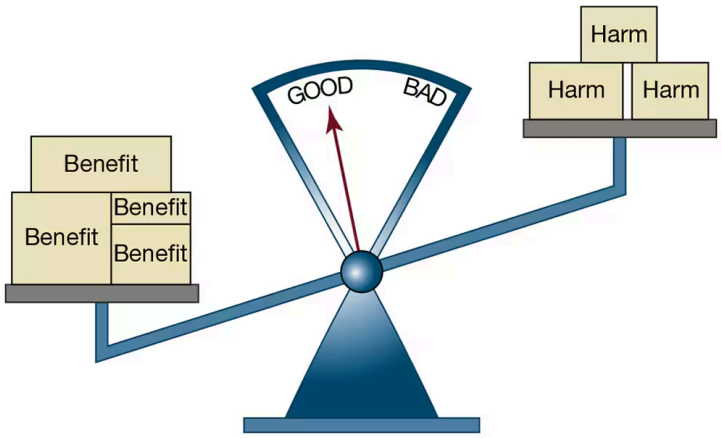
Utility is the tendency of an object to produce happiness or prevent unhappiness for an individual or a community. Depending on the circumstances, you may think of "happiness" as advantage, benefit, good, or pleasure, and "unhappiness" as disadvantage, cost, evil, or pain.

Principle of Utility (Greatest Happiness Principle)

An action is right (or wrong) to the extent that it increases (or decreases) the total happiness of the affected parties.

We can use the principle of utility as a yardstick to judge all actions in the moral realm. Suppose in a particular situation we have a set of possible actions. For each possible action, we must determine, for each affected person, the increase or decrease in that person's happiness and then add up all of these values to reach a grand total: the overall increase or decrease in happiness caused by that particular action (Figure 2.5). We repeat this procedure for every action in the set of possible actions. The moral action is the one that produces the maximum increase in happiness. (If every possible action results in a decrease in happiness, then the moral action is the one that minimizes the decrease in happiness.)

Figure 2.5



Utilitarianism is based on the principle of utility, which states that an actio

Note that the morality of an action has nothing to do with the attitude behind the action. Bentham writes, "There is no such thing as any sort of motive that is in itself a bad one. If [motives] are good or bad, it is only on account of their effects" [21]. We call utilitarianism a **consequentialist** theory, because the focus is on the consequences of an action.

Act utilitarianism is the ethical theory that an action is good if its net effect (over all affected beings) is to produce more happiness than unhappiness. Suppose we measure pleasure as a positive number and pain as a negative number. To make a moral evaluation of an action, we simply add up, over all affected beings, the change in their happiness. If the sum is positive, the action is good. If the sum is negative, the action is bad.

Did you notice that I used the word "beings" rather than "persons" in the previous paragraph? An important decision an act utilitarian must make is determining which beings are

considered to be morally significant. Bentham noted that at one time only adult white males were considered morally significant beings. Bentham felt that any being that can experience pain and pleasure ought to be seen as morally significant. Certainly, women and people of color are morally significant beings by this definition, but in addition all mammals (and perhaps other animals) are morally significant beings, because they, too, can experience pain and pleasure. Of course, as the number of morally significant beings increases, the difficulty of evaluating the consequences of an action also increases. It means, for example, that the environmental impacts of decisions must often be included when performing the utilitarian calculus.

2.7.2 Evaluating a Scenario Using Act Utilitarianism

Scenario

A state is considering replacing a curvy stretch of highway that passes along the outskirts of a large

city. Would building the highway be a good action?

Analysis

To perform the analysis of this problem, we must determine who is affected and the effects of the highway construction on them. Our analysis is in terms of dollars and cents. For this reason we'll use the terms "benefit" and "cost" instead of "happiness" and "unhappiness."

About 150 houses lie on or very near the proposed path of the new, straighter section of highway. Using its power of eminent domain, the state can condemn these properties. It would cost the state $20 million to provide fair compensation to the homeowners. Constructing the new highway, which is three miles long, would cost the taxpayers of the state another $10 million. Suppose the environmental impact of the new highway in terms of lost habitat for morally significant animal species is valued at $1 million.

Every weekday, 15,000 cars are expected to travel on this section of highway, which is one mile shorter than the curvy highway it replaces.

Assuming it costs 40 cents per mile to operate a motor vehicle, construction of the new highway will save drivers $6,000 per weekday in operating costs. The highway has an expected operating lifetime of 25 years. Over a 25-year period, the expected total savings to drivers will be $39 million.

We'll assume the highway project will have no positive or negative effects on any other people. Since the overall cost of the new highway is $31 million and the benefit of the new highway is $39 million, building the highway would be a good action.

Commentary

Performing the benefit/cost (or happiness/unhappiness) calculations is crucial to the utilitarian approach, yet it can be controversial. In our example, we translated everything into dollars and cents. Was that reasonable? Neighborhoods are the site of many important relationships. We did not assign a value to the harm the proposed highway would do to these neighborhoods. There is a good chance that many of the homeowners would be angry about being forced out of their houses,

even if they were paid a fair price for their properties. How do we put a dollar value on their emotional distress? On the other hand, we can't add apples and oranges. Translating everything into dollars and cents is one way to put everything into common units.

Bentham acknowledged that a complete analysis must look beyond simple benefits and harms. Not all benefits have equal weight. To measure them, he proposed seven attributes that can be used to increase or decrease the weight of a particular pleasure or pain:

- *Intensity:* magnitude of the experience
- *Duration:* how long the experience lasts
- *Certainty:* probability it will actually happen
- *Propinquity:* how close the experience is in space and time
- *Fecundity:* its ability to produce more experiences of the same kind

- *Purity:* extent to which pleasure is not diluted by pain or vice versa
- *Extent:* number of people affected

As you can see, performing a complete calculation for a particular moral problem can be a daunting prospect!

2.7.3 The Case For Act Utilitarianism

1. *It focuses on happiness*.

   By relying upon the Greatest Happiness Principle as the yardstick for measuring moral behavior, utilitarianism fits the intuition of many people that the purpose of life is to be happy.

2. *It is practical*.

   The utilitarian calculus provides a straightforward way to determine the right course of action to take. Start by identifying the set of possible alternatives. Next, consider each of the alternatives in turn. For each alternative, total up the anticipated positive and negative consequences to all of the affected parties resulting from the action. Finally, identify the

alternative with the maximum total. That alternative is the right action to take. This process, conducted in an open manner in which all the information is made available to all the key stakeholders, is a good way for a diverse group of people to come to a collective decision about a controversial topic.

For example, suppose your state needs to build a new prison because the number of people who are incarcerated is growing. Everybody understands the prison must be built somewhere in the state, but nobody wants the prison in their neighborhood. A panel of trusted citizens considers a variety of siting options and, after a series of public hearings to gather evidence, weighs the pluses and minuses of each location. At the end of the process, the panel makes public the individual scores and grand totals and recommends the site with the highest grand total. While some will be unhappy at the prospect of a prison being built near their homes, an open and impartial process can speed their acceptance of the decision.

3. *It is comprehensive*.

Act utilitarianism allows the moral agent to take into account all the elements of a particular situation. Do you remember the problem of having to decide what to

say about your mother's awful haircut? Utilitarianism allows you to take into account the emotional distress that telling the truth would cause to you and your mother. That harm could tilt the balance toward telling your mother what she wants to hear.

2.7.4 The Case Against Act Utilitarianism

1. *When performing the utilitarian calculus, it is not clear where to draw the line, yet where we draw the line can change the outcome of our evaluation*.

   In order to perform our calculation of total net happiness produced by an action, we must determine whom to include in our calculation and how far into the future to consider the consequences. In our highway example, we counted the people who lost their homes and the people who would travel the new highway in the next 25 years. The proposed highway may cut neighborhoods in two, making it more difficult for some children to get to school, but we did not factor in consequences for neighbors. The highway may cause people to change their commutes, increasing traffic congestion in other parts of town, but we did not count

those people either. The highway may be in existence for more than 25 years, but we didn't look beyond that date. We cannot include all morally relevant beings for all time into the future. We must draw the line somewhere. Deciding where to draw the line can be a difficult problem.

2. *It is not practical to put so much energy into every moral decision.*

   Correctly performing the utilitarian calculus requires a great deal of time and effort. It seems unrealistic that everyone would go to so much trouble every time they were faced with a moral problem.

   A response to this criticism is that act utilitarians are free to come up with moral "rules of thumb." For example, a moral rule of thumb might be, "It is wrong to lie." In most situations it will be obvious this is the right thing to do, even without performing the complete utilitarian calculus. However, an act utilitarian always reserves the right to go against the rule of thumb if particular circumstances should warrant it. In these cases, the act utilitarian will perform a detailed analysis of the consequences to determine the best course of action.

3. *Act utilitarianism ignores our innate sense of duty.*

Utilitarianism seems to be at odds with how ordinary people make moral decisions. People often act out of a sense of duty or obligation, yet the act utilitarian theory gives no weight to these notions. Instead, all that matters are the consequences of the action.

W. D. Ross gives the following example [22]. Suppose I've made a promise to A. If I keep my word, I will perform an action that produces 1,000 units of good for him. If I break my promise, I will be able to perform an action that produces 1,001 units of good for B. According to act utilitarianism, I ought to break my promise to A and produce 1,001 units of good for B. Yet most people would say the right thing for me to do is keep my word.

Note that it does no good for an act utilitarian to come back and say that the hard feelings caused by breaking my word to A will have a negative impact on total happiness of $-N$ units, because all I have to do is change the scenario so that breaking my promise to A enables me to produce $1{,}001 + N$ units of good for B. We've arrived at the same result: breaking my promise results in 1 more unit of good than keeping my word.

The real issue is that utilitarianism forces us to reduce all consequences to a positive or negative number. "Doing the right thing" has a value that is difficult to quantify.

4. *We cannot predict with certainty the consequences of an action.*

   In doing the utilitarian calculus, we can identify possible consequences of an action, but we may misjudge the certainty, intensity, and duration of these consequences. The action may have other unforeseen consequences that we forget to include in our calculation. These errors may cause us to choose the wrong course of action.

5. *Act utilitarianism is susceptible to the problem of moral luck.*

   As we noted in the previous point, sometimes actions have unforeseen consequences. Is it right for the moral worth of an action to depend solely on its consequences when these consequences are not fully under the control of the moral agent? This is called the **problem of moral luck**.

> Suppose I hear that one of my aunts is in the hospital, and I send her a bouquet of flowers. After the bouquet is delivered, she suffers a violent allergic reaction to one of the exotic flowers in the floral arrangement, extending her stay in the hospital. My gift gave my aunt a bad case of hives and a much larger hospital bill. Since my action had far more negative consequences than positive consequences, an act utilitarian would say my action was bad. That doesn't seem fair.

Two additional arguments have been raised against utilitarianism in general. We'll save these arguments for the end of the section on rule utilitarianism.

While it is not perfect, act utilitarianism is an objective, rational ethical theory that allows a person to explain why a particular action is right or wrong. It joins Kantianism on our list of workable ethical theories we can use to evaluate moral problems.

2.8 Rule Utilitarianism

The weaknesses of act utilitarianism have led some philosophers to develop another ethical theory based on the principle of utility. This theory is called rule utilitarianism. Some philosophers have concluded that John Stuart Mill was actually a rule utilitarian, but others disagree.

2.8.1 Basis of Rule Utilitarianism

Rule utilitarianism is the ethical theory that holds that we ought to adopt those moral rules that, if followed by everyone, lead to the greatest increase in total happiness over all affected parties. Hence a rule utilitarian applies the principle of utility to moral rules, while an act utilitarian applies the principle of utility to individual moral actions.

Both rule utilitarianism and Kantianism are focused on rules, and the rules these two ethical theories derive may have significant overlap. However, the two ethical theories derive

moral rules in completely different ways. A rule utilitarian chooses to follow a moral rule because its universal adoption would result in the greatest net increase in happiness. A Kantian follows a moral rule because it is in accord with the Categorical Imperative: all human beings are to be treated as ends in themselves, not merely as means to an end. In other words, the rule utilitarian is looking at the consequences of the action, while the Kantian is looking at the will motivating the action.

2.8.2 Evaluating a Scenario Using Rule Utilitarianism

Scenario

A worm is a self-contained program that spreads through a computer network by taking advantage of security holes in the computers connected to the network. In August 2003, the Blaster worm infected many computers running the Windows 2000, Windows NT, and Windows XP operating systems. The Blaster worm caused computers it infected to reboot every few minutes.

Soon another worm was exploiting the same security hole in Windows to spread through the Internet. However, the purpose of the new worm, named Nachi, was benevolent. Since Nachi took advantage of the same security hole as Blaster, it could not infect computers that were immune to the Blaster worm. Once Nachi gained access to a computer with the security hole, it located and destroyed copies of the Blaster worm. It also automatically downloaded from Microsoft a patch to the operating system software that would fix the security problem. Finally, it used the computer as a launching pad to seek out other Windows PCs with the security hole.

Was the action of the person who released the Nachi worm morally right or wrong?

Analysis

To analyze this moral problem from a rule-utilitarian point of view, we must think of an appropriate moral rule and determine if its universal adoption would increase the happiness of the affected parties. In this case, an appropriate moral

rule might be the following: “If I can write and release a helpful worm that improves the security of the computers it infects, I should do so.”

What would be the benefits if everyone followed the proposed moral rule? Many people do not keep their computers up to date with the latest patches to the operating system. They would benefit from a worm that automatically removed their network vulnerabilities.

What harm would be caused by the universal adoption of the rule? If everyone followed this rule, the appearance of every new harmful worm would be followed by the release of many other worms designed to eradicate the harmful worm. Worms make networks less usable by creating a lot of extra network traffic. For example, the Nachi worm disabled networks of Diebold ATM machines at two financial institutions [**23**]. The universal adoption of the moral rule would reduce the usefulness of the Internet while the various “helpful” worms were circulating.

Another negative consequence would be potential harm done to computers by the supposedly helpful

worms. Even worms designed to be benevolent may contain bugs. If many people are releasing worms, there is a good chance some of the worms may accidentally harm data or programs on the computers they infect.

A third harmful consequence would be the extra work placed on system administrators. When system administrators detect a new worm, it is not immediately obvious whether the worm is harmful or beneficial. Hence the prudent response of system administrators is to combat every new worm that attacks their computers. If the proposed moral rule were adopted, more worms would be released, forcing system administrators to spend more of their time fighting worms [**24**].

In conclusion, the harms caused by the universal adoption of this moral rule appear to outweigh the benefits. Therefore, the action of the person who released the Nachi worm is morally wrong.

2.8.3 The Case For Rule Utilitarianism

1. *Not every moral decision requires performing the utilitarian calculus*.

   A person who relies on rules of behavior does not have to spend a lot of time and effort analyzing every particular moral action in order to determine if it is right or wrong.

2. *Exceptional situations do not overthrow moral rules*.

   Remember the problem of choosing between keeping a promise to A and producing 1,000 units of good for A, or breaking the promise to A and producing 1,001 units of good for B? A rule utilitarian would not be trapped on the horns of this dilemma. A rule utilitarian would reason that the long-term consequences of everyone keeping their promises produce more good than giving everyone the liberty to break their promises, so in this situation a rule utilitarian would conclude the right thing to do is to keep the promise to A.

3. *Rule utilitarianism solves the problem of moral luck*.

Since it is interested in the typical result of an action, the highly unusual result does not affect the goodness of an action. A rule utilitarian would conclude that sending flowers to people in the hospital is a good action.

4. *Rule utilitarianism reduces the problem of bias*.

   A weakness of act utilitarianism is that it creates the temptation to perform a biased analysis. By asking, "Is it okay for me to do this?" an act utilitarian may conclude the action is acceptable by consciously or unconsciously inflating the personal benefits and/or deflating the anticipated harms to others. In contrast, a rule utilitarian must ask the question, "Is it okay for everyone in a similar circumstance to do this?" The person who answers the latter question is more likely to place appropriate weights on the benefits and harms of the action.

5. *It appeals to a wide cross section of society*.

   Bernard Gert points out that utilitarianism is "paradoxically, the kind of moral theory usually held by people who claim that they have no moral theory. Their view is often expressed in phrases like the

following: ‘It is all right to do anything as long as no one gets hurt,’ ‘It is the actual consequences that count, not some silly rules,’ or ‘What is important is that things turn out for the best, not how one goes about making that happen.’ On the moral system, it is not the consequences of the particular violation that are decisive in determining its justifiability, but rather the consequences of such a violation being publicly allowed” [25]. In other words, an action is justifiable if allowing that action would, as a rule, bring about greater net happiness than forbidding that action.

2.8.4 The Case Against Utilitarianism in General

As we have just seen, rule utilitarianism seems to solve several problems associated with act utilitarianism. However, two criticisms have been leveled at utilitarian theories in general. These problems are shared by both act utilitarianism and rule utilitarianism.

1. *Utilitarianism forces us to use a single scale or measure to evaluate completely different kinds of consequences.*

In order to perform the utilitarian calculus, all consequences must be put into the same units. Otherwise we cannot add them up. For example, if we are going to determine the total amount of happiness resulting from the construction of a new highway, many of the costs and benefits (such as construction costs and the gas expenses of car drivers) are easily expressed in dollars. Other costs and benefits are intangible, but we must express them in terms of dollars in order to find the total amount of happiness created or destroyed as a result of the project. Suppose a sociologist informs the state that if it condemns 150 homes, it is likely to cause five divorces among the families being displaced. How do we assign a dollar value to that unfortunate consequence? In certain circumstances utilitarians must quantify the value of a human life. How can the value of a human life be reduced to an amount of money?

2. *Utilitarianism ignores the problem of an unjust distribution of good consequences.*

   Another criticism of utilitarianism in general is that the utilitarian calculus is solely interested in the total amount of happiness produced. Suppose one course of action results in every member of a society receiving

100 units of good, while another course of action results in half the members of society receiving 201 units of good each, with the other half receiving nothing. According to the calculus of utility, the second course of action is superior because the total amount of good is higher. That doesn't seem right to many people.

A possible response to this criticism is that our goal should be to promote the greatest good to the greatest number. In fact, that is how utilitarianism is often described. A person subscribing to this philosophy might say that we ought to use two principles to guide our conduct: (1) we should act so that the greatest amount of good is produced, and (2) we should distribute the good as widely as possible. The first of these principles is the principle of utility, but the second is a principle of distributive justice. In other words, to "act so as to promote the greatest good to the greatest number" is not pure utilitarianism. The proposed philosophy is not internally consistent, because there are times when the two principles conflict. In order to be useful, the theory also needs a procedure to resolve conflicts between the two principles. We'll talk more about the principle of distributive justice in the next section.

The criticisms leveled at utilitarianism point out circumstances in which it seems to produce the "wrong" answer to a moral problem. However, rule utilitarianism treats all persons as equals and provides its adherents with the ability to give the reasons why a particular action is right or wrong. Hence we consider it a third workable theory for evaluating moral problems, joining Kantianism and act utilitarianism.

2.9 Social Contract Theory

In the spring of 2003, a coalition of military forces led by the United States invaded Iraq and removed the government of Saddam Hussein. When the police disappeared, thousands of Baghdad residents looted government ministries [**26**]. Sidewalk arms merchants did a thriving business selling AK-47 assault rifles to homeowners needing protection against thieves. Are Iraqis much different from residents of other countries, or should we view the events in Baghdad as the typical response of people to a lack of governmental authority and control?

2.9.1 The Social Contract

Philosopher Thomas Hobbes (1588–1679) lived during the English civil war and saw firsthand the terrible consequences of social anarchy. In his book *Leviathan*, he argues that without rules and a means of enforcing them, people would not bother to create anything of value, because nobody could be sure of keeping what they created. Instead, people would

be consumed with taking what they needed and defending themselves against the attacks of others. They would live in "continuall feare, and danger of violent death," and their lives would be "solitary, poore, nasty, brutish, and short" [27].

To avoid this miserable condition, which Hobbes calls the "state of nature," rational people understand that cooperation is essential. However, cooperation is possible only when people mutually agree to follow certain guidelines. Hence moral rules are "simply the rules that are necessary if we are to gain the benefits of social living" [10, p. 141]. Hobbes argues that everybody living in a civilized society has implicitly agreed to two things: (1) the establishment of such a set of moral rules to govern relations among citizens and (2) a government capable of enforcing these rules. He calls this arrangement the **social contract**.

The Franco-Swiss philosopher Jean-Jacques Rousseau (1712–1778) continued the evolution of social contract theory. In his book *The Social Contract*, he writes, "Since no man has any natural authority over his fellows, and since force alone bestows no right, all legitimate authority among men must be based on covenants" [28, p. 53]. Rousseau states that the critical problem facing society is finding a form of association

that guarantees everybody their safety and property, yet enables each person to remain free. The answer, according to Rousseau, is for everybody to give themselves and their rights to the whole community. The community will determine the rules for its members, and each of its members will be obliged to obey the rules. What prevents the community from enacting bad rules is that no one is above the rules. Since everyone is in the same situation, no community members will want to put unfair burdens on others because that would mean putting unfair burdens on themselves.

Social contract theory must deal with the reality that it's easy for an individual to rationalize selfish behavior, as noted earlier in this chapter. How do we prevent people from shirking their duties to the group? Suppose Bill owes the government $10,000 in taxes, but he discovers a way to cheat on his taxes so it appears he owes only $8,000. Bill thinks to himself, "The government gets billions of dollars a year in taxes. So to the government another $2,000 is just a drop in the bucket. But to me, $2,000 is a lot of money." What restrains Bill from acting selfishly and cheating on his taxes is the knowledge that if he is caught, he will be punished. In order for the social contract to function, society must provide not only a system of laws but a system of enforcing the laws as well.

According to Rousseau, living in a civil society gives a person's actions a moral quality they would not have if that person lived in a state of nature. "It is only then, when the voice of duty has taken the place of physical impulse, and right that of desire, that man, who has hitherto thought only of himself, finds himself compelled to act on other principles, and to consult his reason rather than study his inclinations" [28, p. 64].

James Rachels summarizes these ideas in an elegant definition of social contract theory.

Social Contract Theory

> Morality consists in the set of rules, governing how people are to treat one another, that rational people will agree to accept, for their mutual benefit, on the condition that others follow those rules as well [10, p. 145].

Hobbes, John Locke, and many other philosophers of the seventeenth and eighteenth centuries held that all morally significant beings have certain rights, such as the right to life, liberty, and property. Some modern philosophers would add other rights to this list, such as the right to privacy.

There is a close correspondence between rights and duties. If you have the right to life, then others have the duty or obligation not to kill you. If you have a right to free health care when you are ill, then others have the duty to make sure you receive it. Rights can be classified according to the duties they put on others. A **negative right** is a right that another can guarantee by leaving you alone to exercise your right. For example, the right of free expression is a negative right. In order for you to have that right, all others have to do is not interfere with you when you express yourself. A **positive right** is a right that obligates others to do something on your behalf. The right to a free education is a positive right. In order for you to have that right, the rest of society must allocate resources so that you may attend school.

Another way to view rights is to consider whether they are absolute or limited. An **absolute right** is a right that is guaranteed without exception. Negative rights, such as the right to life, are usually considered absolute rights. A **limited**

right is a right that may be restricted based on the circumstances. Typically, positive rights are considered to be limited rights. For example, US states guarantee their citizens the right to an education. However, because states do not have unlimited budgets, they typically provide a free education for everyone up through the 12th grade but require people to pay for at least some of the costs of their higher education.

Proponents of social contract theory evaluate moral problems from the point of view of moral rights. In contrast, Kantians evaluate moral problems from duties or obligations, since Kant argued that rights follow from duties.

2.9.2 Rawls's Theory of Justice

John Rawls (1921–2002) did much to revive interest in social contract theory in the twentieth century. Rawls notes that both cooperative and competitive behavior can be found in every society. People form societies because social cooperation produces more benefits than a situation in which individuals are completely on their own. On the other hand, there is competition regarding how the benefits are divided among the members of society, since everyone would rather

have more than less benefits. To be well ordered, a society must establish the rights and duties of its members and also determine a just way of distributing “the benefits and burdens of social cooperation” [2, p. 4].

How can people agree on what these principles of justice should be, when the natural inclination for each person would be to propose principles that would benefit himself or herself? To prevent people from selfishly promoting their own interests, Rawls proposes a thought experiment: the principles are determined from an original position in which each person is hidden behind a **veil of ignorance**. People must agree to the principles before they know what place they will hold in society; they are ignorant of their sex, race, ethnicity, wealth, intellectual capacity, physical abilities or disabilities, and so on. Rawls claims that agreements reached from this initial condition would be fair because people would not choose principles that would harm them if they turned out to be in a disadvantaged position in society relative to others. He proposes that rational people put behind a veil of ignorance would agree upon the following two principles of justice.

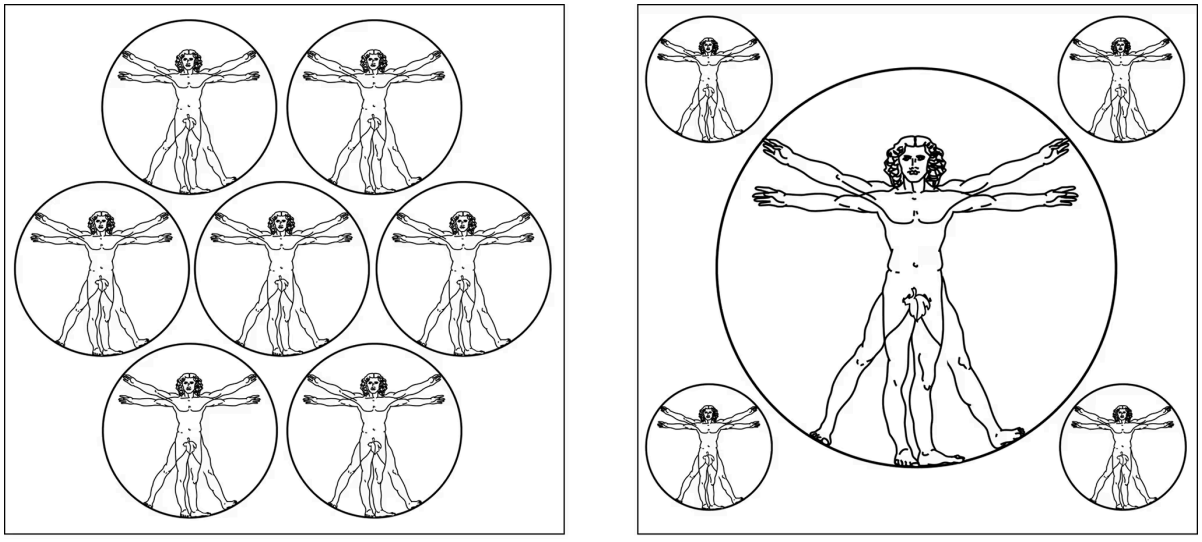
John Rawls's Principles of Justice

1. Each person may claim a "fully adequate" number of basic rights and liberties, such as freedom of thought and speech, freedom of association, the right to be safe from harm, and the right to own property, so long as these claims are consistent with everyone else having a claim to the same rights and liberties.
2. Any social and economic inequalities must satisfy two conditions: first, they are associated with positions in society that everyone has a fair and equal opportunity to assume; and second, they are "to be to the greatest benefit of the least-advantaged members of society (the difference principle)" [**29**, pp. 42–43].

Rawls's first principle of justice, illustrated in Figure 2.6, is quite close to our original definition of social contract theory,

except that it is stated from the point of view of rights and liberties rather than moral rules. The second principle of justice, however, focuses on the question of social and economic inequalities. It is hard to imagine a society in which every person has equal standing. For example, it is unrealistic to expect every person to be involved in every civic decision. Instead, we elect representatives who vote in our place and officials who act on our behalf. Likewise, it is hard to imagine everybody in a society having equal wealth. If we allow people to hold private property, we should expect that some people will acquire more than others. According to Rawls, social and economic inequalities are acceptable if they meet two conditions.

Figure 2.6



Just
(a)

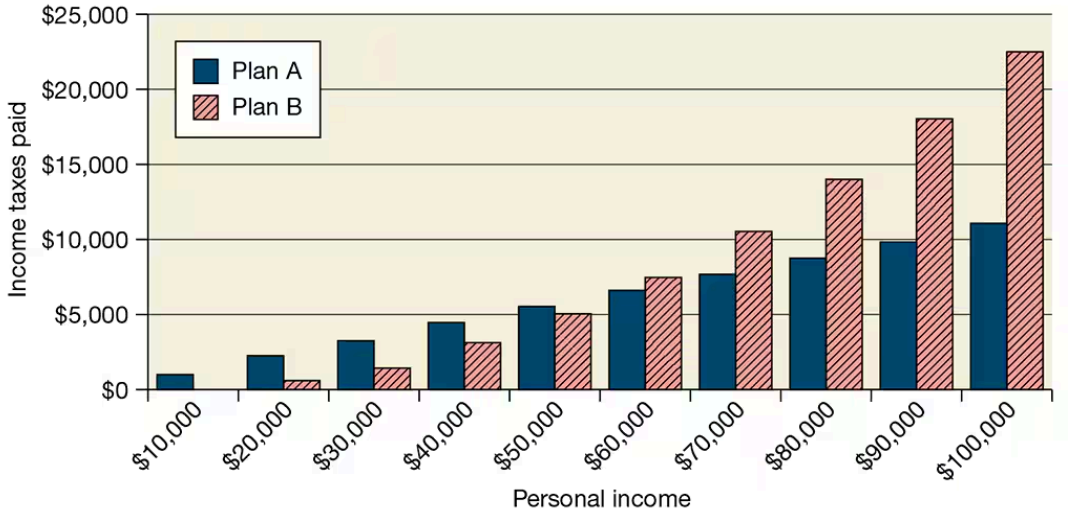
Unjust
(b)

Rawls's first principle of justice states that each person may have a "fully adequate" number of rights and liberties as long as they are consistent with everyone else having the same rights and liberties.

First, every person in the society should have an equal chance to assume a position of higher social or economic standing. That means that two people born with equal intelligence, equal talents, and equal motivation to use them wisely should have the same probability of reaching an advantaged position, regardless of the social or economic class to which they were born. For example, the fact that someone's last name is Bush or Clinton should not give that person a greater probability of being elected president of the United States than any other citizen born with equal intelligence, talent, and determination.

The second condition, called the **difference principle**, states that social and economic inequalities must be justified. The only way to justify a social or economic inequality is to show that its overall effect is to provide the most benefit to the least advantaged. The purpose of this principle is to help maintain a society composed of free *and equal* citizens. An example of the difference principle in action is a graduated income tax system in which people with higher incomes pay a higher percentage of their income in taxes (Figure 2.7). An example of a violation of the difference principle would be a military draft system in which poor people had a higher probability of being drafted than wealthy people.

Figure 2.7



Suppose both of these income tax structures will produce the same income to the government. Plan A is a flat tax in which every citizen pays the same percentage of their income; plan B is a progressive tax in which the income tax rate gradually rises as a citizen's income increases. Plan B does not treat every citizen equally, but the inequality is justified under Rawls's difference principle because it is of greatest benefit to the most disadvantaged.

2.9.3 Evaluating a Scenario Using Social Contract Theory

Scenario

Hao, the owner of a chain of convenience stores, uses a computer to keep track of the items purchased by each customer. Using this information, he is able to construct profiles of the customers: who is responsible for the care of an infant, who owns a pet, who uses a barbeque, etc. Hao sells these profiles to mail-order companies. The customers begin receiving many unsolicited mail-order catalogs. Some of the customers are happy to receive these catalogs and make use of them to order products. Others are unhappy at the increase in the amount of "junk mail" they are receiving.

Analysis

To analyze this scenario using social contract theory, we think about the rights of the rational agents involved. In this case, the rational agents are Hao, his customers, and the mail-order companies. The morality of Hao's actions revolve around the question of whether he violated the privacy rights of his customers. If someone rents a DVD from one of Hao's stores, both the customer and Hao have information about the transaction. Are their rights

to this information equal? If both the customer and Hao have equal rights to this information, then you may conclude there is nothing wrong with him selling this information to a mail-order company. On the other hand, if customers have the right to expect transactions to be confidential, you may conclude that Hao was wrong to sell this information without gaining the permission of the customer.

2.9.4 The Case For Social Contract Theory

1. *It is framed in the language of rights*.

   The cultures of many modern countries, particularly Western-style democracies, promote individualism. For people raised in these cultures, the concept of individual rights is powerful and attractive.

2. *It is based on a solid understanding of human nature, recognizing that rational people act out of self-interest in the absence of a common agreement*.

The **tragedy of the commons** is a modern term used to describe a situation in which individuals benefit from exploiting a resource, while the costs of the exploitation are shared by a community. The term comes from a paper written in England in the 1830s. In medieval England many villages had commons on which herders were allowed to graze their cattle. Sometimes shepherds grazed their sheep on the commons, which was problematic because sheep can overgraze pastures much quicker than cattle. Since an individual shepherd profits from allowing their sheep to overgraze the commons, and no shepherd can save the commons from overgrazing by restraining their sheep if other shepherds allowed their own sheep to overgraze, the rational economic decision for every shepherd is to become a **free rider** and allow their sheep to overgraze the commons. Unfortunately, too many free riders destroy the shared resource and harm the entire community. The way to prevent this consequence is for the community to establish a law against overgrazing, a punishment associated with breaking the law, and a system of law enforcement. Each shepherd will be restrained from acting selfishly by the knowledge that if they are caught, they will be punished.

Social contract theory is based on the idea that morality is the result of an implicit agreement among rational beings who understand that there is a tension between self-interest and the common good. The common good is best realized when everyone cooperates. Cooperation occurs when those acting selfishly suffer negative consequences.

You might ask, "If everyone has a right to liberty, how can we imprison someone who has committed a crime?" The social contract is based on the notion that everyone benefits when everyone bears the burden of following certain rules. Knowledge that those who do not follow the rules will be punished restrains individuals from selfishly flouting their obligations. People will have this knowledge only if society punishes those who commit crimes.

3. *It explains why under certain circumstances civil disobedience can be the morally right decision.*

Consider the lunch counter sit-ins of the 1960s. On February 1, 1960, four African American students from North Carolina A&T walked into the Woolworth's store on South Elm Street in Greensboro, sat down at a whites-only lunch counter, and asked for service. When

they were denied service, they refused to leave, sitting at their stools until the store closed. Two days later, eighty-five students participated in the sit-in at Woolworth's. All of these students were breaking segregation laws, but according to social contract theory, their actions could be considered morally justified. As we have said, the social contract is based on the idea that everyone receives certain benefits in return for bearing certain burdens. The segregation laws were designed to give Black people greater burdens and fewer benefits than white people. Therefore, they were unjust.

2.9.5 The Case Against Social Contract Theory

1. *None of us signed the social contract*.

   The social contract is not a real contract. Since none of us have actually agreed to the obligations of citizens set forth in our society, why should we be bound by them?

   Defenders of social contract theory point out that the social contract is a theoretical notion that is supposed to explain the rational process through which

communities adopt moral guidelines. As John Rawls puts it, social contract agreements are hypothetical and nonhistorical. They are hypothetical in the sense that they are what reasonable people "could, or would, agree to, not what they have agreed to" [**29**, p. 16]. They are nonhistorical because they "do not suppose the agreement has ever, or indeed ever could actually be entered into" [**29**, pp. 16–17]. Furthermore, even if it could be entered into, that would make no difference. The reason it would make no difference is because the moral guidelines are supposed to be the result of analysis (facts and values plus logical reasoning), not history. Social contract theory is *not* cultural relativism in disguise.

2. *Some actions can be characterized in multiple ways*.

   This is a problem social contract theory shares with Kantianism. Some situations are complicated and can be described in more than one way. Our characterization of a situation can affect the rules or rights we determine to be relevant to our analysis.

3. *Social contract theory does not explain how to solve a moral problem when the analysis reveals conflicting rights*.

This is another problem social contract theory shares with Kantianism. Consider the knotty moral problem of abortion, in which the mother's right to liberty is pitted against the fetus's right to life. As long as each of these rights is embraced by one side in the controversy, the issue cannot be resolved. What typically happens in debates is that advocates on one side of the issue "solve" the problem by discounting or denying the right invoked by their adversaries.

4. *Social contract theory may be unjust to those people who are incapable of upholding their side of the contract.*

Social contract theory provides every person with certain rights in return for that person bearing certain burdens. When a person does not follow the moral rules, they are punished. What about human beings who, through no fault of their own, are unable to follow the moral rules?

A response to this objection is that there is a difference between someone who deliberately chooses to break a moral rule and someone who is incapable of understanding a rule. Society must distinguish between these two groups of people. People who deliberately

break moral rules should be punished, but people who cannot understand a rule must be cared for.

However, this response overlooks the fact that distinguishing between these two groups of people can be difficult. For example, how should people who use drugs and who steal to fund their usage habits be treated? Some countries treat their behavior as criminal and imprison them. Other countries consider their behavior an effect of mental illness and treat them as patients in a hospital.

These criticisms demonstrate some of the weaknesses of social contract theory. Nevertheless, social contract theory is logical and analytical. It allows people to explain why a particular action is moral or immoral. According to our criteria, it is a workable ethical theory, joining Kantianism, act utilitarianism, and rule utilitarianism as a way of evaluating moral problems.

2.10 Virtue Ethics

Some moral philosophers criticize Kantianism, utilitarianism, and social contract theory because they ignore what these philosophers consider to be important aspects of living a moral life, including moral education, moral wisdom, family and social relationships, and the role of emotions [30]. Over the past several decades there has been a resurgence of interest in virtue ethics, an ethical theory that accounts for all of these factors.

Unlike Kantianism, utilitarianism, and social contract theory, which grew out of the Enlightenment, virtue ethics can be traced all the way back to ancient China and Greece. Confucianism, dating back to the fifth century BC, emphasizes the importance of the cultivation of virtues and the development of strong moral character in order to live a good life. In Greece, the notion of *arete*, usually translated as **virtue** or excellence, refers to reaching one's highest potential. An influential treatment of virtue appears in Aristotle's *Nicomachean Ethics*, written in the fourth century BC. In this book Aristotle expresses the opinion that the path to true

happiness and genuine flourishing as a human being lies in living a life of virtue [31].

2.10.1 Virtues and Vices

According to Aristotle, there are two kinds of virtues: intellectual virtues and moral virtues. **Intellectual virtues** are those virtues associated with reasoning and truth. **Moral virtues**, often called virtues of character by today's writers, are habits or dispositions formed through the repetition of the relevant virtuous actions (Figure 2.8). For example, you can develop the moral virtue of honesty by habitually telling the truth or performing other honest actions. In this section our primary focus is on the moral virtues.

Figure 2.8

A moral virtue is a deep-seated character trait. Consider someone who possesses the virtue of honesty, for example. An honest person will tell the truth as a matter of course, will be uncomfortable with even the thought of doing something deceitful, and will not appreciate being invited by others to join in a dishonest activity. Morally good people consistently do what is right; it becomes second nature to them.

Note, then, that a moral virtue is not simply a disposition to *act* in a particular way, it is also a disposition to *feel* in a particular way. According to Aristotle, you can tell a lot about someone's character by observing what pleases them and what bothers them. He wrote, "We may even go so far as to state that the man who does not enjoy performing noble actions is not a good man at all. Nobody would call a man just who does not enjoy acting justly, nor generous who does not enjoy generous actions, and so on" [**31** p. 16].

Of course, some moral virtues have a more direct connection to the emotions than others. Courage is a good example of a virtue that has a close connection with the emotions. In order to be courageous, you must be able to moderate your fear.

As noted earlier, a moral virtue is a deep-seated character trait, and character traits take time to become deep-seated. Consider a young Boy Scout who is encouraged by his scoutmaster to take the Boy Scout slogan seriously and "do a good turn daily." The scout initially responds to this encouragement by actively looking for opportunities to help someone each day, not so much because he is interested in being helpful, but because he looks up to his scoutmaster and seeks his praise and approval. The young scout continues doing daily good deeds for family members, friends, and even strangers for a significant period of time. Eventually, he realizes that he has persisted in his practice of doing a good turn daily so that it has become a habit—something so ingrained that he no longer relies upon the compliments of his scoutmaster for motivation. His daily efforts give him a sense of genuine satisfaction. At this point being helpful to others has become second nature to the scout; he has become benevolent.

When someone possessing a virtue does not exercise the virtue, we know there is a good explanation. Suppose Angel is known for her reliability. She does what she says she will do, and she shows up on time for meetings. Everybody knows they can count on Angel. One morning Angel does not show up for a meeting she had promised to attend. When the

others notice her absence, they say, “Something must have happened.” They understand that there must have been an extenuating circumstance that prevented Angel from showing up for the meeting on time.

Summary of Virtue Ethics

A right action is an action that a virtuous person, acting in character, would do in the same circumstances. A virtuous person is a person who possesses and lives out the virtues. The virtues are those character traits human beings need in order to flourish and be truly happy.

Which virtues are those humans need in order to flourish and be truly happy? To some extent that depends on the culture. In Homeric Greece physical courage was prized; settlers of the North American West put a high value on self-reliance; in today’s multicultural society tolerance is important.

However, certain core virtues, such as honesty, justice, and loyalty, seem to be of universal importance.

A **vice** is a character trait that prevents a human being from flourishing or being truly happy. Vices, then, are the opposite of virtues. Aristotle noticed that in many cases two different vices can be associated with a virtue: one corresponding to an excess and the other corresponding to a deficiency. For example, the virtue of courage can be seen as occupying a middle ground between cowardice (having an excess of fear) and rashness (having a deficiency of fear). The virtue of friendliness is somewhere in between quarrelsomeness (being too critical of what others like or what they want to do) and obsequiousness (giving in too easily and not being critical enough of what others like or what they want to do).

Virtue ethics pays particular attention to the agent (the person performing the action) as well as the action (as in Kantianism and social contract theory) and the consequences of the action (as in utilitarianism). A good person does "the right thing at the right time for the right reason" [32].

According to the theory of virtue ethics, moral decision making cannot be reduced to the routine application of a set of rules. That is not to say there is no place for "rules of thumb." In order to develop the virtue of trustworthiness, for

example, it is a good idea to follow the rule of thumb “Keep confidences.” However, under certain circumstances keeping a confidence may not be the right course of action. Moral wisdom or discernment takes precedence over any rule [30].

2.10.2 Making a Decision Using Virtue Ethics

Scenario

Josh is a senior majoring in computer science at a small university. All the seniors in computer science are friends because they have taken most of their computer science courses together. Josh is particularly close to Reggie. Josh and Reggie are from the same city about 200 miles from campus, and Reggie has given Josh rides to and from home a half dozen times at the start and end of school holidays. Notably, Reggie never asked Josh to help pay for the gas on any of these trips, and Josh never offered to do so.

When it is time for seniors to choose partners for their capstone project, no one is surprised when Josh and Reggie end up on the same team. Unfortunately, Josh and the other teammates soon regret inviting Reggie onto their team. Everyone has known Reggie to be hardworking, trustworthy, and reliable, but his father just died in a car accident, and he has lost all interest in school. To make matters worse, Reggie is drinking too much. He doesn't show up for a lot of the team meetings, and the code he produces doesn't meet the specifications. Josh and the other teammates can't persuade Reggie to take the project more seriously, and since they don't have any real control over his behavior, they decide it's easier simply to rewrite Reggie's part of the system themselves. Reggie does contribute his share of the PowerPoint slides, and during the oral presentation he stands up and talks about "his" portion of the code, never mentioning that it was all rewritten by his teammates.

Everyone in the class is supposed to send the professor an email grading the performance of their teammates. The department prides itself on graduating students who have proven they can

work well on software development teams, and students getting negative performance reviews from all their teammates may be forced to repeat the class. Reggie comes to Josh, tells him that he really needs to pass this class because he can't afford to stay in college any longer, and pleads for a good performance review. What should Josh do?

Decision

Josh must decide whether or not to disclose to the professor that Reggie did not even come close to doing his share of the team project, fully aware that a negative performance evaluation may prevent Reggie from graduating. Josh is an honest person, and he has a hard time imagining that he could tell the professor that Reggie did a good job when that is far from the truth. However, Josh is also a just person, and he feels indebted to Reggie, who has done him a lot of favors over the past four years—particularly those free rides to and from his hometown. Josh also feels compassion toward Reggie, who lost his father. It's bad enough to lose a parent, but because of the sudden nature of his

father's death, Reggie didn't even have the chance to say goodbye to him.

90

As he ponders his dilemma, Josh begins to realize that he finds himself in this difficult spot because at several points in the past he didn't step up and do the right thing. He took advantage of Reggie's generosity (and gave in to his own selfish impulses) by taking all those free rides to and from his hometown. If he had paid his share of the gas money, he wouldn't be feeling so obligated toward Reggie. Josh also knows he wasn't a very good friend when he failed to talk with Reggie about how he was feeling about his father's death and how that was affecting his performance on the senior project. Reggie's lack of attention to his schoolwork was definitely out of character, a sign that he was suffering a lot. Josh now understands that he and the other teammates should have had a conversation with the professor in charge of the senior projects when it first became apparent that Reggie was not participating fully as a teammate. An early intervention could have resulted in a completely different outcome.

After reflecting on what he should do, Josh concludes he must be truthful with the professor. However, he will not simply tell the professor that Reggie's performance was mediocre. Josh decides he will also take responsibility for his role in the fiasco by providing a full account to the professor of how his own failure to respond to the situation earlier in the year contributed to the unsatisfactory outcome.

2.10.3 The Case For Virtue Ethics

1. *In many situations it makes more sense to focus on virtues than on obligations, rights, or consequences*. Consider, for example, why it is wrong to steal to satisfy a selfish desire. According to Kantianism, the act is wrong because the person doing the stealing is not treating his or her victims as ends in themselves. According to rule utilitarianism, stealing is wrong because the long-term consequences of everybody stealing all the time would produce more harm than

good. The explanation from the perspective of virtue ethics is much simpler: stealing to satisfy a selfish desire is wrong because it disrupts one's acquisition of the virtue of honesty, an important step toward genuine fulfillment and happiness.

2. *Personal relationships can be morally relevant to decision making*. Recall that utilitarianism, Kantianism, and social contract theory require us to be completely impartial and treat all human beings as equal. This assumption leads to conclusions that are hard for most people to accept. For example, when a couple is faced with the choice between using $10,000 to take their children to Disneyland for a week or feeding 1,000 refugees who are experiencing hunger for a month, the calculus of utility would conclude contributing to the food security of 1,000 people was the better option. When evaluating the same choice from the perspective of virtue ethics, the relationship the couple has with their children is morally relevant. Parents are supposed to be partial toward their own children, and this can be taken into account when determining the best action to take.

3. *Virtue ethics recognizes that our moral decision-making skills develop over time*. People develop moral virtues

by making habits of the appropriate acts. It takes time for a person's character to develop. Moral wisdom is an intellectual virtue that also takes time to develop. Each of us is on the journey from the-person-I-am to the-person-I-am-meant-to-be, and if I am confused about the right action to take in a particular circumstance, I can consult a role model, someone who more fully possesses the virtues I hope to acquire. In many cultures people consult respected elders when they truly want to do the right thing and feel uncertain about the best course of action.

4. *Virtue ethics recognizes the important role that emotions play in living a moral life*. Virtue ethics recognizes that humans are not dispassionate calculating machines. They are flesh-and-blood creatures with feelings, and when things are going right, their feelings and thoughts are in alignment. As noted before, virtuous people do the right things at the right times for the right reasons. They feel satisfied doing good. When faced with difficult decisions, they are deeply affected.

2.10.4 The Case Against Virtue Ethics

1. *Different people may have quite different conceptions of human flourishing*. According to virtue ethics, virtues are character traits that humans need in order to flourish. We do not live in a homogeneous society, and there are a wide variety of perspectives about what character traits lead to the most fulfilling life. If we cannot agree on which character traits are virtues, then we will not be able to agree on what a virtuous person would do in a particular situation. Therefore, the virtue ethics approach is not as powerful as Kantianism, rule utilitarianism, and social contract theory, which identify moral norms that are universally true.

2. *Virtue ethics cannot be used to guide government policy*. Virtue ethics focuses on the agent, a virtuous human being, more than the act or the consequences of the act. Government policy is typically set by government agencies or groups of officials, not individuals. Consider the case brought up in Section 2.7.2, in which a state must decide whether or not to replace a section of highway. An act utilitarian can

determine the monetary costs and benefits of the proposal and reach a conclusion about the better option. Virtue ethics has something to say about the officials involved in the decision—they should be honest, diligent, and prudent, for example—but it has nothing more to contribute to the analysis.

3. *Virtue ethics undermines attempts to hold people responsible for their bad actions*. According to virtue ethics, people are not born virtuous. Instead, intellectual and moral virtues must be acquired over time. To a great extent, the virtues a person attains depends upon how they are raised by their parents, the education they receive, and the community they grow up in. All these things are outside the control of a child. In that case, how can we hold a person responsible if they acquire vices instead of virtues [33]?

These criticisms show that virtue ethics is not perfect. However, virtue ethics does provide a framework for people to analyze moral situations, to reach a conclusion about the right course of action, and to justify the conclusion using logical arguments. Therefore, we determine that virtue ethics is a workable ethical theory, along with Kantianism, act utilitarianism, rule utilitarianism, and social contract theory.

2.11 Comparing Workable Ethical Theories

The divine command theory, ethical egoism, Kantianism, act utilitarianism, rule utilitarianism, social contract theory, and virtue ethics share the viewpoint that moral good and moral precepts are objective. In other words, morality has an existence outside the human mind. Philosophers call this view **ethical objectivism**.

What distinguishes ethical egoism, Kantianism, utilitarianism, social contract theory, and virtue ethics from the divine command theory is the assumption that ethical decision making is a rational process by which people can discover objective moral principles with the use of logical reasoning based on facts and commonly held values. Kantianism, utilitarianism, social contract theory, and virtue ethics explicitly take other people into consideration when defining what makes an action morally correct, which sets these theories apart from ethical egoism. Of all the theories we

have considered, we conclude that Kantianism, act utilitarianism, rule utilitarianism, social contract theory, and virtue ethics are the most workable.

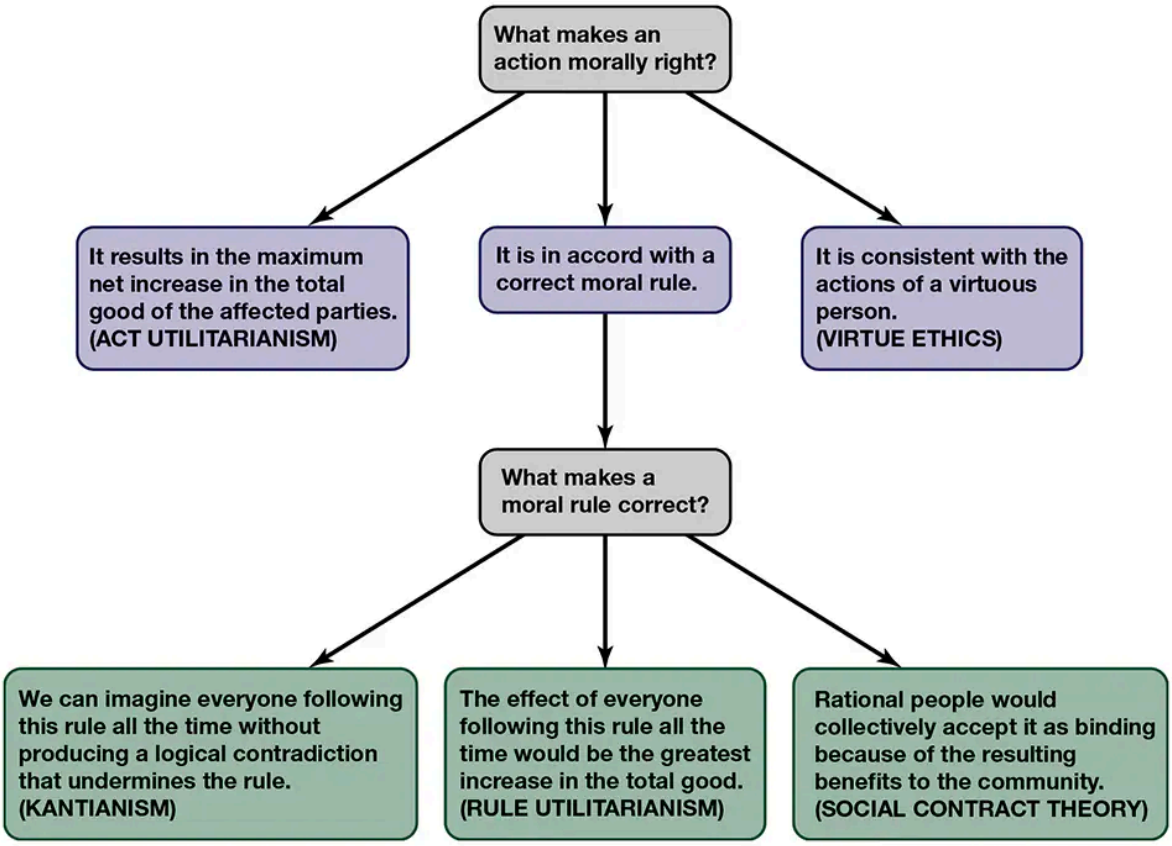
An act utilitarian considers the consequences of the action, computing the total change in utility to determine if an action is good or bad. Kantianism, rule utilitarianism, and social contract theory are rule based. According to these theories, an action is morally right if it is in accord with a correct moral rule.

Each of the rule-based theories has a different way of determining if a moral rule is correct. A Kantian relies upon the Categorical Imperative. A rule utilitarian considers what the long-term consequences of everyone following the rule would be for the total good. An adherent of social contract theory considers whether rational people would agree to accept the rule, for everyone's mutual benefit, provided that everyone else agreed to follow the rule as well.

Unlike the other theories, which focus on the act itself or the consequences of the action, virtue ethics focuses on the agent. The purpose of the analysis is to carefully examine the action taken by an agent in a particular situation to determine if that action is characteristic of a virtuous person.

These differences among the theories are presented graphically in Figure 2.9.

Figure 2.9


What makes an action morally right?
It results in the maximum net increase in the total good of the affected parties. (ACT UTILITARIANISM)
It is in accord with a correct moral rule.
It is consistent with the actions of a virtuous person. (VIRTUE ETHICS)
What makes a moral rule correct?
We can imagine everyone following this rule all the time without producing a logical contradiction that undermines the rule. (KANTIANISM)
The effect of everyone following this rule all the time would be the greatest increase in the total good. (RULE UTILITARIANISM)
Rational people would collectively accept it as binding because of the resulting benefits to the community. (SOCIAL CONTRACT THEORY)

Comparison of the five workable ethical theories. All these theories explicitly take people other than the decision maker into consideration, assume that moral good and moral precepts are objective, and rely upon reasoning from facts and commonly held values.

2.12 Morality of Breaking the Law

What is moral and what is legal are not identical. Certain actions may be wrong, even if there are no laws forbidding these actions. For example, some governments do not have laws prohibiting texting while driving, but drivers are still morally responsible for traffic accidents they cause because they are distracted by texting. What about the opposite situation? Is it possible that an action may be the right thing to do, even if it is illegal?

In our discussion of social contract theory, we talked about the morality of civil disobedience, and we concluded that from the perspective of this theory the lunch counter sit-ins were morally acceptable because the segregation laws being violated were unjust. Here we are considering a different situation. We are assuming the law is just. When this is the case, is it possible that an illegal action may be the right action?

To ground our analysis, we will consider a particular illegal action: violating a licensing agreement by copying a CD

containing copyrighted music and giving it to a friend.[1]

2.12.1 Social Contract Theory Perspective

Social contract theory is based on the assumption that everyone in society ought to bear certain burdens in order to receive certain benefits. The legal system is instituted to guarantee that people's rights are protected. It guarantees people will not choose their selfish interests over the common good. For this reason we have a prima facie obligation to obey the law (Figure 2.10). That means, everything else being equal, we should be law abiding. In return, our own legal rights will be respected. Our obligation to obey the law should be broken only if we are compelled to follow a higher-order moral obligation.

Figure 2.10

From the point of view of social contract theory, then, it is wrong to give a friend a copy of a CD containing copyrighted music, because that action violates the legal rights of the person or organization owning the copyright. The desire to do something nice for a friend is not an overriding moral concern.

2.12.2 Kantian Perspective

The Kantian perspective is quite similar to that of social contract theory. People need to be able to possess objects in order to freely use them for their own purposes. According to Kant, property rights are made possible through an implicit common agreement. When you declare that an object is yours, you are stating that everyone else is obliged to refrain from using that object. Justice demands that in order for you to make such a claim, you must also respect the similar claims of everyone else. The state ensures that everyone meets the obligation of respecting everyone else's property rights.

If you were to copy a CD containing copyrighted material, you would be violating the property rights of the copyright owner—you would be failing to fulfill your obligations to

others as a member of civil society. Therefore, it is wrong to copy the CD.

2.12.3 Rule-Utilitarian Perspective

For a utilitarian, the value of laws lies in their utility. For example, everyone should drive on the same side of the road in order to reduce harmful accidents and improve traffic flow, a benefit. Therefore, it makes sense to pass a traffic law mandating that everyone drive on the same side of the road and indicating the penalties for those who disobey the law. In order to fund social goods such as education, parks, and the arts, governments pass laws governing the taxes everyone must pay.

What would be the consequences of people ignoring laws whenever they chose? A beneficial consequence would be the immediate happiness of the people who are doing what they please rather than obeying the law. However, there would be numerous harmful consequences. The people directly affected by lawless actions would be harmed. People in general would have less respect for the law, which would encourage more people to break the law. Assuming increased lawlessness puts an additional burden on the criminal justice system, society

as a whole would have to pay for having additional police officers, prosecutors, judges, and prisons, reducing the amount of money available to pay for social goods such as schools, parks, and museums. Therefore, according to rule utilitarianism, there are in general strong reasons for obeying the law.

However, it is going too far to assume a rule utilitarian would simply adopt the rule, "Obey the law." Some governments have passed laws that are positively harmful to society. You could argue that the segregation laws in effect in some parts of the United States until the 1960s would be in that category. In certain circumstances the ultimate effect of breaking a law (e.g., through civil disobedience) is the retraction of the bad law and the institution of a new law that has much greater utility. Taking harmful laws into account, a more nuanced moral rule would be, "Obey the law unless (1) the law does not maximize utility, and (2) you have good reason to believe that the long-term net effects of breaking the law will be greater utility."

Does current copyright law maximize utility to society? Copyright law represents a utilitarian compromise between the rights of the creators of intellectual property and those who wish access to it. The public benefits from the artistic

expressions of the creators of intellectual property. The creators of intellectual property benefit by collecting money from those who access their work for a certain period of time. If everyone copied CDs containing copyrighted music, only consumers would derive benefits. Musicians would lose a significant source of income from writing and performing songs, and music publishers would have no reason to continue producing CDs. Both the quantity and quality of music available to consumers could decline significantly. Since it is unclear that the long-term effects of breaking the law will be greater utility, we conclude it is wrong to copy a CD containing copyrighted material.

2.12.4 Act-Utilitarian Perspective

It is possible to conceive of situations where the benefits of breaking a law are greater than the harms. Suppose I purchase a copyrighted music CD. I play it, and I think it is great. A friend of mine is in a terrible automobile accident. While they recover, they will need to stay quiet for a month. I know they have no money to spend on music. In fact, people are doing fund-raisers simply to help their family pay the medical bills. I don’t have money to contribute to a fund-

raiser, but I think of another way I could help them out. I can give my friend a copy of the CD. They will be grateful for having a diversion during their time of bed rest.

What would be the consequences of my action? The benefit to my friend is at least $15, the price of the CD. I will be very happy to have been able to do something that pleased them so much. We assign the value $10 to that beneficial consequence. As far as I can tell, there is no lost sale, because even if I do not give my friend a copy of the CD, they are unlikely to purchase it. In fact, giving a copy of the CD to my friend may actually increase the sales of the CD if my friend likes it and recommends it to other people who do have money to spend on CDs. So there are no negative consequences to the record label and may even be some positive consequences. We assign a value of $0 as the consequence to the record label. I am not likely to be prosecuted for what I did. Therefore, there will be no impact on the criminal justice system. No extra police detectives, prosecutors, or judges will need to be hired as a result of my action. The calculated consequence of my action on the legal system has a value of $0. Adding up all the consequences, the total is $25 worth of benefit. If I do not give my friend a copy of the CD (i.e., do nothing), there are no consequences, so the

total benefit is $0. Therefore, making a copy of the CD and giving it to my hospitalized friend is the right thing to do.

2.12.5 Conclusion

There is nothing intrinsically immoral about copying a CD. However, our society has chosen to enact laws that grant intellectual property rights to people who do creative work and distribute it on CDs. From the perspective of social contract theory and Kantianism, we have a prima facie obligation to obey the law and respect everyone's property rights. From the viewpoint of rule utilitarianism, the beneficial consequences of following the moral rule "Obey the law" greatly exceed the harmful consequences. From the point of view of all these theories, the law should be obeyed unless there is a strong overriding moral obligation. Copying a disc to save a few dollars or help a friend does not fall into that category.

From an act-utilitarian viewpoint, it is possible to come up with a circumstance where making a copy of a copyrighted CD is the right action. However, it would be wrong to extrapolate from this particular case and conclude that an act-utilitarian analysis would always determine CD copying to be morally acceptable.

his action is illegal in the United States and many other countries, but it is no egal in every country.

Summary

We live together in communities for our mutual benefit. Every society has guidelines indicating what people are supposed to do in various circumstances. We call these guidelines morality. Ethics, also called moral philosophy, is a rational examination of people's moral beliefs and behaviors. In this chapter we have considered a variety of ethical theories, with the purpose of identifying those that will be of most use to us as we consider the effects of information technology on society.

Ethical relativism is the idea that people *invent* morality. An ethical relativist claims there are no universal moral principles. Subjective relativism is the theory that morality is an individual creation. Cultural relativism is the idea that each society determines its own morality. If morality is invented, and no set of moral guidelines is any better than another, then there are no objective criteria that can be used to determine if one set of guidelines is better than another. Under these circumstances, the study of ethics is extremely

difficult, if not impossible. You can't do ethics without values.

In contrast, ethical objectivism is based on the idea that morality has an existence outside the human mind. It is the responsibility of people to *discover* morality. An objectivist claims there are certain universal moral principles that are true for all people, regardless of their historical or cultural situation. All the other theories discussed in this chapter are based on ethical objectivism, including the five most practical theories that we will be using throughout the rest of the book: Kantianism, act utilitarianism, rule utilitarianism, social contract theory, and virtue ethics.

Our discussion of the strengths and weaknesses of these practical theories revealed that each of them contains a valuable insight. According to Kant, every human being is equally valuable, and every interaction with another person should respect that person’s rationality and autonomy. Utilitarians understand that it’s helpful to consider the consequences of an action when deciding whether it is right or wrong. Social contract theory focuses on the individual and collective benefits of protecting certain human rights, such as the right to life, liberty, and property. Virtue ethics is

based on the idea that you can count on a good person to do the right thing at the right time in the right way.

Our discussion of these theories also revealed that none of them is perfect. In practice, however, there is no reason why you should not consider virtues *and* duties *and* rights *and* consequences when making moral decisions. If analyses from all of these perspectives result in a consensus on the right course of action, you can make the decision with confidence. For more challenging cases, however, you will find it impossible to come up with a virtuous course of action that respects everyone's rights absolutely and maximizes the total increase in happiness. That's when things get interesting! Most of the scenarios discussed in the rest of the book fall into the latter category.

In the chapters that follow, we'll use Kantianism, act utilitarianism, rule utilitarianism, social contract theory, and virtue ethics to evaluate a variety of situations arising from the introduction of information technology into society. Every analysis will be based on one of the theories, so that you may come to a better understanding of how to apply each theory to different situations. As you ponder these cases and discuss them with others, you will learn more about your

own values, what kind of person you want to be, and what kind of world you want to live in.

Further Reading, Listening, and Viewing

Nathan Colaner. "Rationalization Analysis: Ethics & Artificial Intelligence: Case Analysis." *AI Institute in Dynamic Systems*, Episode 3. Viewed June 5, 2013. 17:46. https://www.youtube.com/watch?v=-bRMENGVmhs.

Jonathan Haidt. "The Moral Roots of Liberals and Conservatives." *TEDTalks*, September 2008. 18:40. www.ted.com/talks/jonathan_haidt_on_the_moral_mind.html.

Damon Horowitz. "We Need a 'Moral Operating System.'" *TEDxSiliconValley*, May 2011. 16:18. www.ted.com/talks/damon_horowitz.

Christopher Shea. "Rule Breaker." *Chronicle of Higher Education*, June 12, 2011. chronicle.com.

Paul Solman. "Finding the Connection Between Prosperity and Happiness." *PBS NewsHour*, June 20, 2013. 9:44. video.pbs.org.

Paul Solman. "'Pernicious' Effects of Economic Inequality." *PBS NewsHour*, June 21, 2013. 9:24.

video.pbs.org.

Thomas Sowell. “The Fallacy of ‘Fairness.’” Creators.com, February 8, 2010. www.creators.com.

“Rationalizations.” *Ethics Unwrapped, McCombs School of Business*, University of Texas. 1:53. https://ethicsunwrapped.utexas.edu/glossary/rationalizations.

Review Questions

1. Define in your own words what "the ethical point of view" means.
2. What is the difference between ethical relativism and ethical objectivism?
3. Two people are debating the morality of a particular action. Person A explains why they believe the action is wrong. Person B disagrees with person A. Their response is, "That's your opinion." Person B has not made a strong ethical argument. Why not?
4. What do we mean when we say an ethical theory is rational?
5. What is the many/any fallacy? Invent your own example of this fallacy.
6. Come up with your own example of a moral rule that would violate the Categorical Imperative.
7. What is plagiarism? Describe four different ways that a person can commit plagiarism. (See Appendix A.)

8. What is the difference between plagiarism and misuse of sources?

9. What is the difference between a consequentialist theory and a nonconsequentialist theory?

10. Give three examples of a situation in which your action would be primarily motivated by a sense of duty or obligation. Give three examples of a situation in which your action would be primarily motivated by its expected consequences.

11. Create your own example that demonstrates the problem of moral luck.

12. Why do businesses and governments often use utilitarian thinking to determine the proper course of action?

13. Think of a real-life law or policy that violates the difference principle.

14. Is social contract theory as first presented a consequentialist theory or a nonconsequentialist theory? Is social contract theory as articulated in Rawls's two principles of justice a consequentialist theory or a nonconsequentialist theory?

15. Come up with a list of 20 virtues not mentioned in Section 2.10.
16. Describe similarities and differences between subjective relativism and ethical egoism.
17. Describe similarities and differences between divine command theory and Kantianism.
18. Describe similarities and differences between subjective relativism and act utilitarianism.
19. Describe similarities and differences between Kantianism and rule utilitarianism.
20. Describe similarities and differences between act utilitarianism and rule utilitarianism.
21. Describe similarities and differences between cultural relativism and social contract theory.
22. Describe similarities and differences between Kantianism and social contract theory.
23. Describe similarities and differences between cultural relativism and virtue ethics.
24. Evaluate the four scenarios presented in Section 2.1.3 from a Kantian perspective.

25. Evaluate the four scenarios presented in Section 2.1.3 from an act-utilitarian perspective.

26. Evaluate the four scenarios presented in Section 2.1.3 from a rule-utilitarian perspective.

27. Evaluate the four scenarios presented in Section 2.1.3 from the perspective of social contract theory.

28. Evaluate the four scenarios presented in Section 2.1.3 from the perspective of virtue ethics.

Discussion Questions

29. In *The Portrait of Dorian Gray*, Oscar Wilde wrote: "Conscience and cowardice are really the same thing" [34]. In other words, the fear of getting caught is the only thing that stops people from doing bad things. Do you agree?

30. If everyone agreed to take the ethical point of view by respecting others and their core values, would there be any need for a rigorous study of ethics?

31. If you had to choose only one of the ethical theories presented in this chapter and use it for all your personal ethical decision making, which theory would you choose? Why? How would you respond to the arguments raised against the theory you have chosen?

32. Most ethical theories agree on a large number of moral guidelines. For example, it is nearly universally held that it is wrong to steal. What difference, then, does it

make whether someone subscribes to the divine command theory, Kantianism, utilitarianism, or one of the other ethical theories?

33. Suppose a spaceship lands in your neighborhood. Friendly aliens emerge and invite humans to enter the galactic community. You learn that this race of aliens has colonized virtually the entire galaxy; Earth is one of the few inhabitable planets to host a different intelligent species. The aliens seem to be remarkably open-minded. They ask you to outline the ethical theory that should guide the interactions between our two species. Which ethical theory would you describe? Why?

34. The Silver Rule states, "Do not do unto others what you do not want them to do unto you." Which of the five workable ethical theories is closest to the Silver Rule?

35. According to the Golden Rule, you should do unto others as you would want them to do unto you. Which of the five workable ethical theories is closest to the Golden Rule?

36. Are there any ethical theories described in this chapter that would allow someone to use the argument

"Everybody is doing it" to show that an activity is not wrong?

37. How well does Moor's theory of just consequentialism (described in the interview at the end of this chapter) solve the problems associated with Kantianism and rule utilitarianism?

38. Can moral decisions be made on a completely codified, algorithmic basis, or are there fundamental weaknesses to this approach to moral decision making?

39. What are some examples of contemporary information technology issues for which our society's moral guidelines seem to be nonexistent or unclear? (Hint: Think about issues that are generating a lot of media coverage.)

40. People give a variety of reasons for copying a music CD from a friend instead of buying it [35]. Refute each of the reasons given below, using one of the viable theories described in this chapter. (You don't have to use the same theory each time.)

    a. I don't have enough money to buy it.

    b. The retail price is too high. The company is gouging customers.

c. Since I wouldn't have bought it anyway, the company didn't lose a sale.

d. I'm giving my friend the opportunity to do a good deed.

e. Everyone else is doing it. Why should I be the only person to buy it when everyone else is getting it for free?

f. This is insignificant compared to the billions of dollars made by some people who illegally sell copied music

g. This is insignificant compared to the billions of dollars' worth of music being exchanged over the Internet.

41. Students in a history class are asked to take a quiz posted on the course Web site. The instructor has explained the following rules to the students: First, they are supposed to do their own work. Second, they are free to consult their lecture notes and the textbook while taking the quiz. Third, in order to get credit for the quiz, they must correctly answer at least 80 percent of the questions. If they do not get a score of 80

percent, they may retake the quiz as many times as they wish.

Latoya and Omar are both taking the quiz. They are sitting next to each other in the computer room. Omar asks Latoya for help in answering one of the questions. He says, "What's the difference if you tell me the answer, I look it up in the book, or I find out from the computer that my answer is wrong and retake the quiz? In any case, I'll end up getting credit for the right answer." Latoya tells Omar the correct answer to the question.

Discuss the morality of Latoya's decision.

42. Suppose a society holds that it is wrong for one individual to eavesdrop on the telephone conversations of another citizen. Should that society also prohibit the government from listening in on its citizens' telephone conversations?

In-Class Exercises

43. In Plato's dialogue *The Republic*, Glaucon argues that people do not voluntarily do what is right [**36**]. According to Glaucon, anyone who has the means to do something unjust and get away with it will do so. Glaucon illustrates his point by telling the story of Gyges.

    Gyges, a shepherd, finds a magic ring. He accidentally discovers that wearing this ring renders him invisible. He uses the power of the ring to seduce the queen, kill the king, and take over the kingdom.

    Divide the class into groups of about four students each. Each group should discuss the following proposition: Whenever people have the opportunity to act unjustly without any fear of getting caught or anyone thinking the worse of them, they do so. After a reasonable length of time, groups should take turns sharing their conclusions with the rest of the class.

44. Divide the class into groups of about four students each. Each group is assigned one of the following rights

and should discuss whether that right should be considered a legitimate positive right by our society. After a reasonable length of time, groups should take turns sharing their conclusions with the rest of the class. The rights to be discussed are:

a. The right to a higher education

b. The right to housing

c. The right to health care

d. The right of a presidential candidate to receive time on television

45. Is the right to life a negative right or a positive right? In other words, when we say someone has the right to life, are we simply saying we have an obligation not to harm that person, or are we saying we have an obligation to provide that person with what they need in order to live, such as food and shelter?

Divide the class into groups of about four students each. Half the groups should come up with reasons why the right to life should be considered a negative right, and the remaining groups should come up with reasons why the right to life should be considered a positive right. After a reasonable length of time, groups should

take turns sharing their reasons with the rest of the class.

46. Divide the class into two groups (pro and con) to debate this proposition: The citizens of a representative democracy are morally responsible for the actions of their government.

47. Divide the class into two groups (pro and con) to debate this proposition: The moral guidelines for individuals should apply to interactions among nation-states.

References

[1] James H. Moor. “Reason, Relativity, and Responsibility in Computer Ethics.” In *Readings in CyberEthics*. 2nd ed., edited by Richard A. Spinello and Herman T. Tavani. Jones and Bartlett, Sudbury, MA, 2004.

[2] John Rawls. *A Theory of Justice*. Revised Edition. Belknap Press of Harvard University Press, Cambridge, MA, 1999.

[3] Chris Melore. “Nearly Half of Americans Think They’re a Better Person than EVERYONE They Know!” StudyFinds (website), May 6, 2021. https://studyfinds.org/half-americans-think-better-person-than- everyone/.

[4] “In It to Win: Jack and Rationalizations.” *McCombs School of Business*, University of Texas, 4(37), November 12, 2012. https://ethicsunwrapped.utexas.edu/video/jack-rationalizations.

[5] “Rationalizations.” *Ethics Unwrapped*, *McCombs School of Business*, University of Texas, 1(53).

https://ethicsunwrapped.utexas.edu/glossary/rationalizations.

[6] "Rationalization." *The Cambridge Dictionary of Philosophy*. Robert Audi, editor. Cambridge University Press, Newyork, USA, 1999.

[7] Nathan Colaner. "Rationalization Analysis: Ethics & Artificial Intelligence: Case Analysis." Video. *AI Institute in Dynamic Systems*, Episode 3, 17(46), Viewed June 5, 2023. https://www.youtube.com/watch?v=-bRMENGVmhs.

[8] Plato. *Portrait of Socrates: Being the Apology, Crito and Phaedo of Plato in an English Translation*. Translated by Sir R. W. Livingstone. Clarendon Press, Oxford, England, 1961.

[9] William Graham Sumner. *Folkways: A Study of the Sociological Importance of Usages, Manners, Customs, Mores, and Morals*. Ginn and Company, Boston, MA, 1934.

[10] James Rachels. *The Elements of Moral Philosophy*. 4th ed. McGraw-Hill, Boston, MA, 2003.

[11] Plaut W. *The Torah: A Modern Commentary*. Union of American Hebrew Congregations, New York, NY, 1981.

[**12**] *The Holy Bible, New Revised Standard Version.* Genesis, Chapter 22. Oxford University Press, Oxford, England, 1995.

[**13**] *The Holy Bible, New Revised Standard Version.* Genesis, Chapter 4. Oxford University Press, Oxford, England, 1995.

[**14**] Ayn Rand. "The Objectivist Ethics." In *The Virtue of Selfishness*. p. 1, Signet Books, New York, NY, 1964.

[**15**] Douglas Birsch. *Ethical Insights: A Brief Introduction.* 2nd ed. McGraw-Hill, Boston, MA, 2002.

[**16**] James Rachels. "Two Arguments Against Ethical Egoism." *Philosophia*, 4(2–3): 297–314, April–July 1974.

[**17**] James H. Fowler and Nicholar A. Christakis. "Dynamic Spread of Happiness in a Large Social Network: Longitudinal Analysis over 20 Years in the Framingham Heart Study." *British Medical Journal*, 337(a2338): 1–9, December 4, 2008.

[**18**] Lewis White Beck. "Translator's Introduction." In *Foundations of the Metaphysics of Morals*. P. vii-xxiv, 2nd ed. Library of Liberal Arts/Prentice Hall, Upper Saddle River, NJ, 1997.

[19] Michael J. Sandel. *Justice: What's the Right Thing to Do?* Farrar, Straus and Giroux, New York, NY, 2009.

[20] William K. Frankena. *Ethics*. 2nd ed. Prentice Hall, Englewood Cliffs, NJ, 1973.

[21] Jeremy Bentham. *An Introduction to the Principles of Morals and Legislation*, p. 48. Clarendon Press, Oxford, England, 1823.

[22] W. D. Ross. *The Right and the Good*. 2nd ed. Oxford University Press, Oxford, England, 2003.

[23] Kevin Poulsen. "Nachi Worm Infected Diebold ATMs." *Register*, November 25, 2003. www.theregister.co.uk.

[24] Florence Olsen. "Attacks Threaten Computer Networks as Students Arrive For the Fall Semester." *Chronicle of Higher Education*, 50(2): A42, September 5, 2003.

[25] Bernard Gert. "Common Morality and Computing." In *Readings in CyberEthics*. 2nd ed., edited by Richard A. Spinello and Herman T. Tavani, p. 106. Jones and Bartlett, Sudbury, MA, 2004.

[26] John Daniszewski and Tony Perry. "War with Iraq; U.S. in Control; Baghdad in U.S. Hands; Symbols of

Regime Fall as Troops Take Control." *Los Angeles Times*, April 10, 2003.

[27] Thomas Hobbes. *Leviathan*, p. 186. Penguin Books, London, England, 1985.

[28] Jean-Jacques Rousseau. *The Social Contract*. Translated by Maurice Cranston. Penguin Books, London, England, 1968.

[29] John Rawls. *Justice as Fairness: A Restatement*. Belknap Press of Harvard University Press, Cambridge, MA, 2001.

[30] Rosalind Hursthouse. *On Virtue Ethics*, pp. 2–3. Oxford University Press, Oxford, England, 1999.

[31] Aristotle. *The Nicomachean Ethics*. Translated by F. H. Peters and M. Ostwald. Oxford University Press, Oxford, England, 1998.

[32] John Bradshaw. *Reclaiming Virtue: How We Can Develop the Moral Intelligence to Do the Right Thing at the Right Time For the Right Reason*. Bantam Books, New York, 2009.

[33] Nafsika Athanassoulis. "Virtue Ethics." In *The Internet Encyclopedia of Philosophy*, July 7, 2010.

www.iep.utm.edu.

[34] Oscar Wilde. *The Picture of Dorian Gray*, p. 14. Bernhard Tauchnitz, Leipzig, 1908.

[35] Sara Baase. *A Gift of Fire*. 2nd ed. Prentice Hall, Upper Saddle River, NJ, 2003.

[36] Plato. *The Republic of Plato*. Translated by F. M. Cornford. Oxford University Press, London, England, 1941.

Chapter 3

Networked Communications

3.1 Introduction

ON THE EVENING OF SEPTEMBER 6, 2022, THE CELLPHONES OF 27 million californians simultaneously blared an alarm. It wasn't an Amber Alert, though. Instead, the text read: "Power interruptions may occur unless you take action." An extreme heat wave had increased power consumption in the state to 52,000 megawatts, and the electrical grid was maxed out. Fortunately, the emergency text message worked where ordinary appeals had failed. Within 45 minutes, residents reduced their power consumption by 2,600 megawatts, and rolling blackouts were averted [**1**].

M- Pesa, Africa's first mobile money platform, allows people to conduct financial transactions using their mobile phones. Millions of Africans who have never had a bank account use their cell phones to save money, pay bills, and transfer funds over large distances. In Kenya, where nearly every household has an M-PESA account, access to mobile money has reduced poverty by encouraging saving and supporting entrepreneurship. Nearly 200,000 Kenyan women have used

M-PESA to raise their families' incomes by shifting from subsistence farming to business or sales occupations [2].

In 2017 the Royal Society for Mental Health interviewed 14–24-year-olds in the United Kingdom to better understand how their use of social media affected their mental health and sense of well being. The survey revealed that 91 percent of young people used social media sites. The report noted some positive effects from the use of social media: allowing young people to grow real-world relationships; serving as a vehicle for positive self-expression; providing the opportunity to learn about other people's mental health issues and experiences; and delivering emotional support during difficult times. However, the report also warned that the heavy use of social media can have detrimental effects on the mental health of young people, by increasing feelings of anxiety, lowering the quality of sleep, raising concerns about body image, exposing them to cyberbullying, and heightening the fear of missing out [3].

Before the 2016 presidential election, more than 100 pro-Trump Web sites were being managed from Veles, a small town in Macedonia. The Macedonians were not Trump supporters, but they found the creation of these sites to be an easy way to make money. They plagiarized stories from right-

wing sites in the United States, added sensationalized headlines, posted the stories to their sites, and then used the "share" feature of Facebook to generate traffic to the stories. When people clicked on their stories, Google paid them for the ads placed on their pages [4].

Watching other people compete at video games, or **eSports**, began with the Internet café culture in South Korea and China and has now become a global phenomenon. Professional eSports leagues are growing in popularity, and companies throughout North America are transforming movie theaters, parking garages, and other large spaces into eSports arenas. Twitch is the most popular platform for live streaming video games over the Internet. The most popularly watched eSports event in 2022 was the League of Legends World Championship, which attracted more than 5 million viewers [5].

These stories illustrate how the Internet and cellular networks are changing life in the modern world (Figure 3.1). The development of these networks has provided us with exciting new ways to conduct business, connect with friends, and entertain ourselves. However, other fruits of the same technologies are bitter: new ways of scamming people, new

ways to bully and harass others, and new concerns about the impact of social media on democratic institutions.

Figure 3.1

Far more people in the world have access to cellphones than to electricity or clean water.

(Charles Sturge/Alamy Stock Photo)

In this chapter we explore how people use and abuse the Internet and cellular networks. We discuss how people communicate with one another and how they organize and find information. Some governments are threatened by the way in which modern networks have supported these activities; we detail various kinds of censorship and consider appropriate limits to the freedom of expression. We also discuss and evaluate new behaviors that have emerged with the growth of these networks, such as sexting, cyberbullying, and Internet addiction.

3.2 Spam

Over 4 billion people around the world use email, and every day about 350 billion email messages are sent [**6**]. Unfortunately, a significant percentage of this traffic consists of unsolicited bulk email, or **spam**.

Why is spam called spam? Brad Templeton, chairman of the board of the Electronic Frontier Foundation, traces the term back to the SPAM sketch from *The Final Rip Off* by Monty Python's Flying Circus, in which a group of Vikings drown out a café conversation by loudly and obnoxiously repeating the word "spam" [7]. In a similar way, legitimate email messages can get "drowned out" by spam.

3.2.1 The Spam Tsunami

The rise of spam corresponded with the transformation of the Internet from a noncommercial academic and research enterprise into a commercial global network. Early spam messages provoked Internet users and generated big headlines. For example, in 1994 Phoenix lawyers Laurence Canter and Martha Siegel sent an email advertising their immigration services to more than 9,000 electronic

newsgroups. Canter and Siegel received tens of thousands of responses from outraged newsgroup users who did not appreciate seeing an off-topic, commercial message. The *New York Times* reported the incident with the tongue-in-cheek headline, "An Ad (Gasp!) in Cyberspace." Canter and Siegel were undeterred. Their ad was successful in bringing them new clients. "We will definitely advertise on the Web again," Canter said. "I'm sure other businesses will be advertising on the network in the very near future" [8]. Still, spam was not seen as much of a problem throughout the 1990s, and even in the year 2002 it accounted for only about 9 percent of all email traffic [9].

The spam tsunami hit in 2003, with a big jump in the volume of spam messages, and by 2009 about 85 percent of all email messages were spam [10]. Spam consumed a large percentage of the Internet's bandwidth and huge amounts of storage space on mail servers and individual computers.

To deal with the deluge, an entire industry grew up developing software designed to filter out spam. These filters looked for a large number of messages coming from the same email address, messages with suspicious subject lines, or messages with spamlike content. ISPs and businesses installed spam filters to keep spam from reaching users' mailboxes.

Even with spam filters in place, the cost to businesses in wasted productivity from the spam that got through was estimated at tens of billions of dollars per year in the United States alone [**11**].

The volume of spam grew so large because spam is effective. The principal advantage of spam is its low cost compared to other forms of advertising. For about $10, a company can send an advertisement to a million different email addresses [**12**]. Sending the same advertisement to a million addresses using the US Postal Service costs at least $40,000 for the mailing list and $280,000 for bulk-rate postage. And that doesn't include the cost of the brochures! In other words, an email advertisement is more than 30,000 times cheaper than a traditional flyer sent out in the mail.

Where do spammers get email lists with millions of addresses? The Internet provides a variety of sources of email addresses that can be harvested and sold to spammers. For example, email addresses often appear in Web sites, in chat-room conversations, and newsgroups. Some computer viruses gather email addresses stored in the address books of PCs and transmit these addresses to spammers.

Another way to garner email addresses is through dictionary attacks (also called directory harvest attacks). Spammers

bombard Internet service providers (ISPs) with millions of emails containing made-up addresses, such as AdamA@isprovider.com, AdamB@isprovider.com, AdamC@isprovider.com, and so on. Of course, most of these emails will bounce back, because the addresses are no good. However, if an email doesn't bounce, the spammer knows there is a user with that email address and adds it to its mailing list.

Sometimes people voluntarily reveal their email address. Have you ever entered a contest on the Web? There is a good chance the fine print on the entry form said you agree to receive "occasional offers of products you might find valuable" from the company's marketing partners; in other words, spam [**13**]. Sign-ups for email lists often contain this fine print, too.

At the peak of the spam tsunami in 2009, about 90 percent of spam was being sent out by **botnets**: huge networks of compromised computers controlled by "bot herders." Bot herders create botnets by launching programs that search the Internet for computers with inadequate security and install software robot programs, called bots, on these vulnerable systems. A computer with the bot program installed on it is called a zombie because it can be directed by a remote

computer to perform certain tasks. Bot herders can send out billions of email messages every day by dividing the address lists among the hundreds of thousands of zombies they control [**14**].

For more than a decade, law enforcement agencies and Internet service providers around the world have engaged in a sustained effort to shut down botnet command centers [**15**]. In addition, the behavior of spammers appears to have changed after 2009, moving away from scattershot mailings to somewhat more selective email lists [**15**]. For both these reasons, the share of spam in email traffic peaked at around 85 percent in 2009 and has been trending downward ever since [**10**]. In 2022 spam accounted for about 49 percent of all email messages [**16**].

3.2.2 Need for Social–Technical Solutions

As we saw in Chapter 1, new technologies sometimes cause new social situations to emerge. The spam epidemic is an example of this phenomenon. The Internet allows people to send email messages for virtually no cost. Because a spammer's profits increase as the number of sent messages

increases, every spammer has an incentive to send as many messages as possible.

The spam problem arose because the Internet and email technology developed without taking social expectations into account. The design of the Internet allows sophisticated users to disguise their own email addresses. Spammers take advantage of this loophole to send out millions of messages, knowing that unhappy recipients will not be able to respond. This is contrary to a fundamental social expectation: fairness. In order to be fair, communications should be two-way, not one-way [17].

3.2.3 Case Study: Anh the Acme Accountant

Anh is an accountant at Acme Corporation, a medium-sized firm with 50 employees. All the employees work in the same building, and Anh knows all of them on a first-name basis. In fact, Anh distributes paychecks to Acme's employees at the end of every month.

Anh's 10-year-old daughter is a Girl Scout. During the annual Girl Scout cookie sale, Anh sent an email to all the other Acme employees, inviting them to stop by her desk

during a break and place orders. (There is no company rule prohibiting the use of the email system for personal emails.) Nine of the recipients were happy to get Anh's email, and they ordered an average of four boxes of cookies, but the other 40 recipients did not appreciate having to take the time to read and delete an unwanted message; half of them complained to a coworker about Anh's action.

Did Anh do anything wrong?

Kantian Analysis

According to the second formulation of the Categorical Imperative, we should always respect the autonomy of other people, treating them as ends in themselves and never only as the means to an end. The story provides evidence that Anh was not simply "using" her coworkers as the means to her end of making money for the Girl Scouts. She didn't misrepresent what she was doing. She didn't force anyone to buy the cookies or even read the entire email; employees not interested in Girl Scout cookies could simply delete Anh's message as soon as they read the subject line. Some people who received the email freely chose to buy some cookies. Therefore, what Anh did wasn't strictly wrong.

On the other hand, if Anh had found a way for those people interested in hearing about the Girl Scout cookie drive to "opt in" to her announcement, those people not interested in purchasing Girl Scout cookies would not have been bothered by her email. An "opt in" approach would have been better because it would have shown more respect for the time of Anh's coworkers.

Act-Utilitarian Analysis

We will do our evaluation in terms of dollars and cents, quantifying the benefits and costs of Anh's action. Let's begin with the benefits. A box of cookies costs $4 and provides $3 of profit to the Girl Scouts. Someone who buys a box of Girl Scout cookies understands it is a fund-raising activity and is happy with what they receive for $4. Since the cost of $4 is matched with $4 of benefit, they cancel each other out in our analysis, and we do not have to worry about this factor anymore. The average employee who participated in the sale purchased four boxes of cookies. Nine employees participated, which means Anh sold 36 boxes of cookies and provided $108 of benefit to the Girl Scouts.

Now let's look at the harms. The principal harm is going to be the time wasted by Acme's employees. Anh took orders

and made deliveries during coffee or lunch breaks, rather than on company time, so our focus is on the 40 employees who did not appreciate getting Anh's solicitation. It's reasonable to assume that they spent an average of 15 seconds reading and deleting the message. That adds up to 10 minutes of lost productivity.

Half of the employees spent 5 minutes complaining about what Anh did with a coworker. You can imagine the typical conversation. "What makes her so special?" "How does she get away with this kind of thing?" "If I did this for my kid, I'd get in trouble." Taking both the employee's time and the coworker's time into account, Acme loses 10 minutes of productivity for each conversation. Multiplying 10 minutes by 20 conversations gives us 200 minutes.

)

The total time wasted equals 210 minutes or 3.5 hours. Assume the average Acme employee makes $20 per hour. The cost of the lost productivity is 3.5 hours times $20 per hour or $70.

The benefit of $108 exceeds the cost of $70, so we may conclude that Anh's action was good. We should note, however, that all the benefit went to the Girls Scouts and all the cost was borne by Acme Corporation. It would be perfectly reasonable if the owners of Acme Corporation

concluded that this kind of activity was not in the best interests of the company and created a new policy forbidding the use of company email for cookie drives and other fund-raisers.

Rule-Utilitarian Analysis

What would the consequences be if everyone used the company email system to solicit donations to their favorite causes? All the employees would receive many more messages unrelated to business. There would be plenty of grumbling among employees, lowering morale. Reading and deleting these solicitations would waste people's time, a definite harm. It's unlikely that any one cause would do well if everyone was trying to raise money for their own charity. There is a good chance the owner would become aware of this problem, and a logical response would be to ban employees from sending out this kind of solicitation. Because the harms are much greater than the benefits, it is wrong to use the company email system to solicit donations to a charity.

Social-Contract-Theory Analysis

Acme Corporation does not have a prohibition against using the company's email system for personal business. You could say that by sending out her email solicitation, Anh was

exercising her right to free speech. Of course, she did it in a way that many people might find obnoxious, because even if they did not choose to read her entire message, they had to take the time to scan the subject line and delete it. Unlike spammers, however, Anh did not disguise her identity as the sender, thereby providing unhappy recipients with the opportunity to respond to her email and voice their disapproval of her solicitation. If many of the 40 people who did not appreciate receiving her email sent a reply communicating their displeasure, then Anh got a taste of her own medicine by having to wade through a bunch of unwanted email messages, and she may choose a better method of advertising the Girl Scout cookie drive next year. From a social-contract-theory point of view, Anh did nothing wrong.

Virtue-Ethics Analysis

Good coworkers exhibit many virtues, including honesty, dependability, fairness, friendliness, and respect for coworkers. Three that seem particularly important for this case study are honesty, fairness, and respect. Anh demonstrated honesty by being completely straightforward about the Girl Scout cookie drive with her fellow employees. However, it wasn't fair or respectful for Anh to use the email

system to promote her own daughter's fund-raiser when other employees have not used email for similar solicitations for their children. Anh clearly exercised poor judgment when she sent the email, since half of the company's employees felt the need to complain about it.

Looking at this scenario from a completely different angle, we consider Anh in her role as a parent. Good parents want what is best for their children, and Anh was undoubtedly thinking of her daughter's welfare when she decided to sell the Girl Scout cookies at her workplace. Perhaps her daughter has a quota to meet, or perhaps nice prizes are given to those who sell enough cookies. Viewed in this light, Anh's actions seem consistent with those of a loving parent. However, parents are also supposed to teach their children how to develop into capable and independent adults. Anh could have used the cookie sale as an opportunity to teach her daughter some of those lessons. After all, her daughter is 10 years old, certainly old enough to handle many of the tasks. Instead, Anh ran the entire cookie sale operation herself and simply handed her daughter the proceeds.

We conclude Anh demonstrated many, but not all, of the characteristics of a good coworker and a good parent in this episode. If Anh wanted to help her 10-year-old daughter sell

cookies, fine, but she should have found a way for her daughter to play a more active role in the cookie sale at Acme Corporation. For example, her daughter could have come in after school one day to deliver the cookies to the people who ordered them and collect their payments. In this way, Anh's daughter could have gained the satisfaction of knowing she had contributed a good portion of the time and effort needed to achieve the desired result. Furthermore, Anh should have found another way to advertise the sale that respected her workplace's culture of keeping the email system free from solicitations.

Summary

Although the analyses of Anh's action from the perspectives of these five ethical theories reached different conclusions, our analyses have shown she could have taken another course of action that would have been much less controversial. Since Anh has only 49 coworkers, it would not have been too difficult for her to find out who wanted to be notified the next time the Girl Scouts were selling cookies. She could have put a sign-up sheet on her desk or the company bulletin board, for example. By notifying only those people who signed up, Anh's emails would have been solicited and personal. She could still take advantage of the efficiency of

the email system without anyone objecting that she was "using" coworkers or contributing to lost productivity, meaning there would be much less chance of the company instituting a policy forbidding the use of its email system for fund-raising activities. Finally, Anh could have found a way to share the work with her daughter.

3.3 Internet Interactions

The Internet mediates communications and commerce among more than four billion people. In this section we review just a few of the myriad ways people are using the Internet to interact with others and gain access to information.

3.3.1 The World Wide Web

The creation of the World Wide Web stimulated a tremendous growth in the popularity of the Internet. Its creator, Tim Berners-Lee, initially proposed the Web as a documentation system for CERN, the Swiss research center for particle physics, but the creation of easy-to-use Web browsers made the Web accessible to “ordinary” computer users as well [18]. The Web is a hypertext system: a flexible database of information that allows Web pages to be linked to each other in arbitrary fashion.Web browsers such as Chrome, Edge, Safari, and Firefox allow people to traverse this hypertext system with ease.

Two attributes enabled the Web to become a global tool for information exchange. First, it is decentralized. An individual or organization can add new information to the Web without asking for permission from a central authority. Second, every object on the Web has a unique address. Any object can link to any other object by referencing its address. A Web object's address is called a **URL** (uniform resource locator).

3.3.2 Mobile Apps

People are spending more time on smartphones and tablets and less time on laptop or desktop computers. Using Web browsers on mobile devices can be awkward, and for this reason organizations produce **mobile apps**: software programs that are loaded onto mobile devices. Some mobile apps are stand-alone programs, but others connect to the Internet, allowing people to download and upload data. Mobile apps are a popular way to access the Internet because they can be optimized to make the best use of a mobile device's resources (limited screen size, touch interface, etc.) [19].

3.3.3 How We Use the

Internet

Intuitive Web browsers and mobile apps have made the Internet accessible to people with little or no formal computer training. Today billions of people access the Internet for a wide variety of purposes. Here are just a few examples of how people are using the Internet.

1. *We buy*.

   Shopping sites enable us to view and order merchandise from the comfort of our homes. According to the US Census Bureau, ecommerce represented 15 percent of all retail sales in the United States in the first quarter of 2023 [**20**].

2. *We sell*.

   Craigslist allows people to place free classified advertisements on the Internet. Begun by San Franciscan Craig Newmark in 1999, Craigslist is now available in about 90 countries and attracts about 50 billion page views a month [**21**].

3. *We socialize*.

   The Internet has become a popular way for friends to keep in touch with each other. The most popular social

network is Facebook, with 3 billion monthly active users in January 2023 [**22**]. Another well-known social network is LinkedIn, which serves people looking for professional contacts.

In 2012 the Dutch airline KLM launched a program that allows ticketed passengers who have uploaded information from their Facebook or LinkedIn profiles to select seatmates based on the profiles provided by other passengers [**23**].

4. *We contribute content.*

Popular apps allow people to upload videos, photos, podcasts, or other digital content. Instagram, with 2 billion monthly users, allows its users to upload photos and videos and share them on social networking services, such as Facebook.

A **wiki** is a Web site that allows multiple people to contribute and edit its content. The most famous wiki is *Wikipedia*, an online encyclopedia. Relying on the submissions of hundreds of thousands of volunteers, *Wikipedia* has become by far the largest encyclopedia in the world. Seventy-six languages are represented by at least 100,000 articles, but by far the most popular language is English, with more than 6.6 million articles

written as of 2023. However, critics wonder about the quality of a reference work that allows anyone with a Web browser to contribute [**24**].

5. *We blog.*

   A **blog** (short for "Web log") is a personal journal or diary kept on the Web. Used as a verb, the word blog means to maintain such a journal. Blogs may contain plain text, images, audio clips, or video clips [**25**].

   Some commentators use the term **Web 2.0** to refer to a change in the way people use the Web. Social networking services, wikis, Flickr, Reddit, and blogs illustrate that hundreds of millions of people are now using the Web not simply to access content but to build communities and upload and share content they have created.

6. *We visit secret Web sites.*

   A **darknet** is a network of Web sites that can only be accessed through special software that encrypts messages and provides users with anonymity. Darknets are popular with those who have something to hide: people who engage in pedophilia, sell illegal drugs, traffic in illegal weapons, and the like. However, Edward Snowden's disclosure of surveillance by the

National Security Agency has prompted some people to ponder whether everybody should be using darknets on the principle that the government should not be spying on law-abiding citizens [**26**].

7. *We engage in crowdsourcing*.

   Crowdsourcing is an online method of getting goods or services from a large group of people.

   The Waze app is an example of information crowdsourcing. People use Waze to find the quickest way to drive from one place to another. If they allow the app to run while they are driving, it sends their car's GPS coordinates to Waze, which computes vehicle speeds and then uses this information about traffic congestion to help other Waze users find the best route [**27**].

   Financing a project through crowdsourcing is called **crowdfunding**. Kickstarter is an American corporation that supports crowdfunding. Since 2009, more than 22 million people have pledged over $7 billion to successfully fund more than 242,000 projects in a wide variety of creative areas: music, film and video, games, publishing, art, design, technology, theater, comics, food, fashion, and more [**28**].

8. *We learn*.

   When the COVID-19 pandemic struck, schools and universities shifted to online learning, and the popularity of Zoom skyrocketed.

9. *We explore our roots*.

   In the past, genealogists interested in accessing US immigration and census records had the choice between mailing in their requests and waiting for them to be processed or visiting the National Archives and examining the documents by hand. Now FamilySearch.org offers free access to indexes to US census information from 1790 to 1950, allowing genealogical research to be performed remotely—and much more quickly—over the Internet.

10. *We enter virtual worlds*.

    An **online game** is a game played on a computer network that supports the simultaneous participation of multiple players. The Internet enables people to play games with total strangers and makes it possible for aficionados of obscure games to find opponents. The most popular online games attract millions of players.

South Koreans have enjoyed eSports for decades. Cybercafés (called **PC bangs** in South Korea) have large-screen monitors enabling spectators to watch the game-play, which is full of virtual violence and mayhem. Some children spend up to 10 hours a day playing games, hoping to turn professional. Kim Hyun Soo, chairman of the Net Addiction Treatment Center, complains that "young people are losing their ability to relate to each other, except through games" [**29**]. We discuss the topic of Internet addiction in Section 3.11.

The phenomenon of global online gaming has created a real economy based on virtual worlds. In 2005 the *New York Times* reported on Chinese "gold farmers" who worked 12 hours a day, 7 days a week, earning $3,000 a year killing monsters, harvesting virtual gold coins and artifacts, creating powerful avatars, and selling them over the Internet [**30**]. More recently, many citizens of Venezuela, trying to survive in a highly inflationary economy, have turned to gold farming. A Venezuelan gold farmer playing Runescape can earn 12,000 Venezuelan bolivares ($0.50) an hour, five times the minimum wage [**31**].

11. *We control the Internet of Things.*

An increasing number of non-IT devices—thermostats, appliances, lights, motion sensors, door locks, garage-door openers, and baby monitors, to name just a few examples—are being equipped with wireless connections to the Internet, forming an **Internet of Things**. These devices can be controlled from a Web browser, allowing people to oversee them even when they are not at home.

More significantly, some Internet-connected devices can be programmed to interact with each other without human intervention. Imagine devices at home that can monitor the GPS coordinates of the owner's smartphone. An individual could drive home after a long, hot day at work. When they are 15 minutes away from home, the air conditioning in their home turns on. They turn onto their street, and their outdoor light turns on. As they pull into their driveway, the garage door opens automatically [32].

12. *We pay our taxes*.

    About 94 percent of Americans' federal income tax returns for tax year 2021 were filed online [33].

13. *We gamble*.

Internet gambling is a $94 billion-a-year global business [**34**].

14. *We take humanitarian action*.

Kiva is a Web site supporting person-to-person microlending. Kiva works with microfinance institutions to identify entrepreneurs from communities with relatively little wealth, and it posts information about these entrepreneurs on its Web site. People who wish to make an interest-free loan are able to identify the particular person to whom they would like to lend money. Lenders have the ability to communicate with the entrepreneurs and see the impact their loans are having on the recipients, their families, and their communities [**35**].

3.4 Cryptocurrencies

3.4.1 Features of Cryptocurrencies

The Internet has supported the development of **cryptocurrencies**: virtual currencies independent of any bank or government. Bitcoin, released in 2009, was the first cryptocurrency. There are now more than 19,000 cryptocurrencies, and more than 40 of them had market capitalizations of at least $1 billion in 2022, although Bitcoin dominates the other cryptocurrencies. Its market capitalization is nearly as large as that of all the other cryptocurrencies put together [**36**].

The primary features of a cryptocurrency are:

- *Global Accessibility*: Anyone with an Internet connection can send and receive cryptocurrency.
- *Decentralization*: All transactions are recorded in an encrypted public ledger distributed across many

Internet-connected computers.

- *Anonymity*: Cryptocurrency transactions are recorded using a digital address rather than a personal identifier.
- *Security*: To deter fraud and counterfeiting, transactions and the creation of new currency are encrypted.
- *Limited Supply*: The number of coins that can be produced is limited, supporting the value of the cryptocurrency.

3.4.2 Uses of Cryptocurrencies

Cryptocurrencies offer a way for people to make anonymous purchases, which makes cryptocurrencies a popular vehicle for illegal transactions. Since cryptocurrencies are not connected to bank accounts, they are more difficult for law enforcement agencies to seize [37].

Cryptocurrencies are popular in Africa, Southeast Asia, and Latin America as a way for overseas workers to transfer funds back to their families [38]. Two countries have recognized cryptocurrencies as legal tender: El Salvador in 2021 and the Central African Republic in 2022.

The most popular use of cryptocurrencies is as an investment vehicle. Many people engage in speculation, purchasing cryptocurrencies in the hope that their value will rise. Some people see cryptocurrencies as a hedge against inflation.

3.4.3 Sustainability Concerns

Cryptocurrencies are supported by decentralized networks of computers. Because there is no central authority, the group of computers must agree by consensus about all cryptocurrency transactions. Distributed computers reach consensus using a formal protocol.

The encrypted, distributed ledger of cryptocurrency transactions is called a **blockchain**. **Proof of work** is a consensus protocol used to add blocks to a blockchain. To deter an attacker from creating a false blockchain, the proof-of-work protocol requires a large amount of cryptographic work to be performed to create a new block. **Block miners** running hash algorithms on special-purpose computers compete to generate the next block. When one block miner discovers a valid hash, other miners in the network verify the hash is correct. Discovering the hash takes a tremendous

computational effort; verifying the hash is correct is quick [**39**]. The winning block miner is paid for their effort in the virtual currency plus fees for the transactions in the new block [**40**]. Bitcoin and most other cryptocurrencies rely upon the proof-of-work protocol to maintain their blockchains.

In the case of Bitcoin, a new block is added to the blockchain about once every 10 minutes. The amount of electricity used to generate a new block is astonishing. A single Bitcoin transaction has a carbon footprint equal to the carbon footprint of more than 750,000 Visa credit-card transactions. The annual electrical consumption associated with all Bitcoin transactions is comparable to the electrical consumption of the Netherlands [**41**]. As one of its efforts to save energy, China took steps in 2021 to end cryptocurrency mining within its borders [**42**].

The enormous carbon footprint of cryptocurrencies that rely on the proof of work protocol has heightened interest in another consensus protocol called proof of stake. **Proof-of-stake** protocols use validators instead of miners. By "staking" some of its cryptocurrency as collateral, a validator gets a chance to earn cryptocurrency by validating some new transactions. The algorithm randomly selects validators based on how much they have staked. The more a validator stakes,

the greater its chances of being selected. When a validator validates a good transaction, it earns cryptocurrency. If a validator validates a transaction that other validators determine to be fraudulent, it may lose some of its collateral as punishment [**43**, **44**].

Compared to proof of work, proof of stake has the advantage that it doesn't require many computational operations to validate a transaction, making it a more environmentally responsible option. The reduced computational requirements should enable cryptocurrencies using the proof-of-stake protocol to handle far more transactions per second than cryptocurrencies relying on the proof-of-work protocol. The primary disadvantage of proof of stake is that the protocol has not yet demonstrated it is as secure from attacks as the proof-of-work protocol [**43**, **44**].

In September 2022, Ethereum, the second largest cryptocurrency by total market capitalization, switched from proof-of-work mining to proof-of-stake mining, reducing its electrical consumption by an estimated 99.8 percent [**45**].

3.4.4 Financial Concerns

A variety of financial concerns have been raised about Bitcoin

and other cryptocurrencies.

Bitcoin is the dominant cryptocurrency, but only 3–7 Bitcoin transactions per second can be performed worldwide. In comparison, VisaNet can process more than 24,000 Visa transactions per second [**46**]. There is no way Bitcoin will ever replace credit cards for everyday transactions.

Cryptocurrency prices are volatile, making them a highly speculative investment vehicle. For example, the price of one Bitcoin was about $1,000 in April 2017, $65,000 in November 2021, $16,000 in November 2022, and $70,000 in March 2024.

Many Nobel-prize-winning economists have declared Bitcoin to be an economic bubble. Angus Deaton said, “The only advantage as far as I can see is you can be a crook. You don’t want to leave any record. It’s not an accident that people who demand ransoms demand them in Bitcoin” [**47**].

Since the launch of Bitcoin in 2009, over 2,000 other cryptocurrencies have failed. Many of these currencies were outright frauds or scams. Others were based on poor business plans [**48**]. If a cryptocurrency exchange goes bankrupt, no government protects the cryptocurrency deposits. In

November 2022 the cryptocurrency exchange FTX Trading filed for bankruptcy [**49**].

The proof-of-work protocol is not immune from cyberattacks. If a hacker gains control of a majority of a system's hash rate in a so-called **51% attack**, the hacker can alter events and insert double transactions, allowing the same digital coin to be spent more than once. The Digital Currency Initiative at MIT has detected dozens of 51% attacks on various cybercurrencies [**50**].

It is unclear how long governments will refrain from regulating cryptocurrencies. China was the largest cryptocurrency market, but in September 2021 the government of China made all cryptocurrency transactions illegal [**51**].

3.5 Text Messaging

Text messaging greatly increases the versatility of cell phones as information-sharing platforms. Some of the most impressive uses of text messaging are in countries where people do not have easy access to the Internet, banks, and other services taken for granted by those in countries with more infrastructure.

3.5.1 Transforming Lives in Areas with Limited Infrastructure

Text- message-based services such as M-PESA in Kenya allow people in areas with limited infrastructure to save money and pay bills using their cell phones, bypassing traditional banks. To pay a bill or transfer funds to a friend, the user simply types a text message that the recipient is able to turn into cash at any M-PESA office.

For the past decade, Kenya's Agricultural Commodities Exchange has partnered with Safaricom to provide information about crop prices to farmers via a text-messaging

service. Another service, iCow, uses voice and text messaging to help dairy farmers keep track of the gestation of their cows [52].

Counterfeit medicine is a serious problem in many African and Asian countries. Ghanian Bright Simons came up with the idea of putting scratch cards with unique codes on packages of medicine. After scratching the package to reveal the code, a customer can text the code to a designated number to learn if the drug is genuine [52].

3.5.2 Twitter

Twitter is a Web-based social networking service that allows its users to send out text messages known as **tweets**. The service is popular because people who want their friends to know what they are doing find it more convenient to post a single tweet than to type a bunch of text messages. Many people also use Twitter as a blogging tool; they make their tweets public so that anyone can read them. Other Twitter members never post tweets, but they sign up to follow the tweets posted by other people they are interested in.

More than 200 million people use Twitter regularly [53]. Users posted a record 580,166 tweets per minute during the

World Cup Final soccer match between Germany and Brazil in 2014 [54].

3.5.3 Business Promotion

When carpenter Curtis Kimball started a part-time business running a crème brûlée cart in San Francisco, he used Twitter to let people know the cart's location and the flavors of the day. Before long, he had attracted 5,400 followers. Business became so good he quit his day job in order to keep up with demand. Many tiny businesses with no money for advertising rely upon Twitter as their only marketing tool [55].

3.6 Political Impact of Social Media and Online Advertising

3.6.1 Political Activism

Text messaging played an important role in the ousting of the president of the Philippines, Joseph Estrada, in 2001. During his impeachment trial, his political allies in the Philippine congress voted to keep some evidence against him from being revealed. Filipinos who hoped to see President Estrada convicted used text messaging to organize a demonstration on Epifanio de los Santos Avenue in Manila. Over the next couple of days, millions more text messages were sent and forwarded—many reading "Go 2 EDSA. Wear blk."—and the crowd rose to more than one million people. Intimidated by the size of the protest, Estrada's supporters in the Philippine congress changed their votes and allowed the incriminating evidence against President Estrada to be released. Within hours, Estrada's presidency was over [56].

Ten years later, Twitter and Facebook played a highly visible role in the "Arab Spring" demonstrations that led to revolutions in Tunisia and Egypt, a civil war in Libya, and protests in many other Arab countries. In the midst of the protests in Cairo in 2011 that led to the resignation of President Hosni Mubarak, one protester tweeted, "We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world" [57]. Arab news organization Al Jazeera created a "Twitter Dashboard" indicating the level of tweeting activity in many Arab nations where there was unrest [58].

Scholars of the Arab Spring uprisings point to an interesting phenomenon: People started using online social networks such as Twitter in order to keep up with their friends, but these interactions caused them to become politicized. Through these networks, bloggers met new people, became exposed to new ideas, and developed an interest in human rights [59].

Others think the role of social media in catalyzing social change has been overblown. They argue that social networks like Twitter and Facebook are great at building networks of people with weak connections to each other, but high-risk

activism requires strong ties among the members of a hierarchical organization [**60**].

The Arab Spring uprisings demonstrate how Twitter can support grassroots activism. However, Twitter can also be used by a single person or small organization to give the false impression of grassroots support of a political candidate and to trick the Google search engine into prominently featuring misinformation. Here's an early example of such an effort. In 2010 Massachusetts held a special election to fill its vacant US Senate seat. Someone supporting the Republican candidate created nine fake Twitter accounts and used them to send 979 tweets to 573 users in about two hours. Each of these tweets included the URL of a Web site containing misinformation about the Democratic candidate. These tweets were retweeted 143 times and reached 61,732 Twitter users. Google's real-time search engine detected the rapidly growing interest in the URL and promoted the URL to the top of its results page for the Democratic candidate. In other words, for a period of time anyone who typed the name of the Democratic candidate into the Google search engine received as the top result the URL of the Web page containing misinformation about that candidate [**61**].

Social media played a significant role in the protests following the murder of George Floyd in Minneapolis, Minnesota, on May 25, 2020. Police officers had arrested Mr. Floyd for allegedly passing a counterfeit $20 bill in a convenience store [**62**]. When 17-year-old bystander Darnella Frazier saw police officers pinning Mr. Floyd to the ground outside the store, she began filming the incident on her smartphone [**63**]. The video clearly showed white police officer Derek Chauvin choking Mr. Floyd, who was Black, by putting his knee on Mr. Floyd's neck until Mr. Floyd was dead. The heartbreaking video, posted to Facebook, prompted Black Lives Matter protests across the United States. Between 15 and 26 million Americans marched in these protests, making it the largest protest movement in US history [**64**]. All four Minneapolis police officers were fired. Mr. Chauvin was convicted of murder and sentenced to 22.5 years in prison. The other three officers received prison sentences of several years [**62**].

Social media played an important role in the events surrounding the January 6, 2021, occupation of the US Capitol by protesters objecting to the outcome of the 2020 US presidential election. The Republican candidate was President Donald Trump, and the Democratic candidate was Joe Biden. Early in the morning of November 4, while votes

were still being counted, President Trump tweeted that Democrats were "trying to STEAL the Election" [**65**]. An hour-and-a-half later, he called the election results fraudulent [**65**]. Later that day, the first Stop the Steal group was formed on Facebook. The group quickly grew to 320,000 followers before Facebook deleted it [**66**]. Facebook ended up shutting down hundreds of similar groups. Eventually, pro-Trump supporters began shifting their activities to more permissive social media sites, such as Parler and Gab. Those two sites became the center of the movement to organize a protest on January 6, 2021, the date Congress was scheduled to certify the election results [**66**]. President Trump made several tweets between late December and early January, encouraging people to attend a protest in Washington, DC, on January 6 [**66**]. Right-wing groups used social media to communicate plans regarding bringing weapons into Washington, DC, and penetrating the Capitol Building [**67**]. At noon on January 6, President Trump held a "Save America" rally during which he called on his supporters to go to the Capitol [**68**]. Thousands of protesters marched to the Capitol. Between 2,000 and 2,500 people crossed the police line, entered the Capitol, and disrupted the vote certification process for hours [**69**]. Eventually, about 700 people were charged with federal crimes for their participation in the riot. Ironically, FBI agents used social media posts to identify many of the rioters,

and some rioters received harsher sentences because of self-incriminating evidence they had posted on social media [70].

)

3.6.2 Macedonian Entrepreneurs

Among US corporations, Meta (which owns Facebook) and Google are the two giants in online advertising revenue [71]. Facebook is popular among advertisers because it has a huge user base and allows advertisers to target their ads to categories of Facebook users based on various demographics, such as age, income level, locale, religion, sexual orientation, and political leanings.

Google's digital advertising offerings include contextual advertising, which places advertisements on Web pages if the content of those pages is algorithmically determined to be closely related to the advertisement. Through Google's AdSense program, people can make money from their Web pages by allowing Google to place advertisements in them. Google determines the advertisements that are displayed, and the Web site owner receives a monthly check from Google based on the number of people who clicked on the ads.

Both Meta and Google make money when people click on links leading to pages containing advertising. “Nothing drives clicks better than when the headline is exactly what people want to hear or believe,” says Ian Schafer, founder of the digital advertising agency Deep Focus [**72**]. Capitalists hoping to share in the advertising revenue stream know this too.

As mentioned at the beginning of the chapter, a group of young Macedonians leveraged Facebook and Google to make a lot of money for themselves in the run-up to the 2016 US presidential election. At one point, more than 100 pro-Trump Web sites were being managed from Veles, Macedonia. The Macedonians registered their sites with Google’s AdSense program, then made them attractive to visitors by copying stories from conservative Web sites in the United States, adding their own sensationalized headlines, and using Facebook’s “share” feature to drive traffic to their pages. When people clicked on their stories, Google paid them for the ads placed on their pages. The most popular stories, such as the false account that Pope Francis had endorsed Donald Trump for president, were shared by hundreds of thousands of Facebook users. Web site curators who got in on the action early made up to $5,000 per month, a substantial sum in Macedonia [**4**].

3.6.3 Internet Research Agency

The Internet Research Agency (IRA), based in St. Petersburg, Russia, employs hundreds of people who use social media to exert political influence in other countries. In February 2018, a grand jury for the District of Columbia returned a 37-page indictment charging the IRA, two other Russian organizations, and 13 Russian nationals (ten of them employed by the IRA) with interfering in the US presidential election of 2016, in violation of US law. According to the indictment, the Russians set up social media accounts in the United States using false US personas. Posing as Americans, the Russians posted inflammatory material to social media sites and organized rallies with the intent of helping the campaign of Donald Trump and harming the campaign of Hillary Clinton [73].

The grand jury indictment provided evidence that in addition to the short-term goal of promoting Donald Trump and undermining Hillary Clinton, the IRA's long-term goal was to increase political polarization in the United States. According to the indictment, after Donald Trump was elected president, IRA employees helped organize both pro-Trump

and anti-Trump rallies for the same day in New York City [73].

About a year after the election, Facebook released an estimate that the IRA published about 80,000 posts that reached the news feeds of about 29 million American Facebook users between 2015 and 2017. Another 97 million Americans received the posts after other Facebook users clicked “like” or “share” or commented on Russian-created posts. About 10 million Americans saw advertisements purchased by the IRA [74].

Since the election, many have asked whether the “fake news” stories posted by the IRA were responsible for Donald Trump’s victory. One study concluded that “fake news most likely did have a substantial impact on the voting decisions of a strategically important set of voters” [75], but another study concluded that social media may have played only a marginal role in influencing voters [76].

3.6.4 Is Democracy Being Threatened?

Whether or not the Russian misinformation campaign changed the outcome of the 2016 US presidential election, is

it possible that the widespread use of social media is threatening the pillars of democratic societies by undermining trust, “informed dialogue,” and “a shared sense of reality” [77]? In its quest to maximize its revenue, Meta wants to keeps its Facebook users engaged. That means feeding them content they are interested in reading or viewing. To do this, Facebook builds profiles of user preferences and then feeds news stories and other data to users aligning with their preferences. The result is the segregation of Facebook users into ideological “echo chambers” [77].

Two- thirds of US adults read news stories on social media sites, and Facebook is by far the most popular of them, providing nearly half of US adults with at least some of their news [78]. Facebook’s algorithms help ensure people will get news stories that confirm their views, rather than expose them to alternative narratives.

Nearly two decades ago, Cass Sunstein argued that information technology could weaken democracy by allowing people to filter out news that contradicts their view of the world [79]. Today, Sunstein’s words seem prophetic. However, in one crucial respect the environment is even more insidious than what Sunstein described. Sunstein assumed that people would be actively choosing to view Web sites or

watch cable channels that confirmed their opinions. In the world moderated by Facebook, people aren't actively making the choices; instead, they are passively receiving the content delivered to them by Facebook's algorithms.

3.6.5 Troubling Times for Traditional Newspapers

The rapid growth in advertising through social media and the popularity of Craigslist have weakened the financial health of traditional print newspapers. "Craigslist came up with a new model for classified ads—free—with which newspapers could not compete" [80]. Advertising revenues for print newspapers dropped from $44.9 billion in 2003 to $16.4 billion in 2014 [81]. Although newspapers began selling digital advertisements, their revenues of $3.5 billion in 2014 from online ads did not come close to making up for the $28.5 billion decline in revenues from printed advertisements they had experienced [81].

Newspapers that had been making lots of money in prior decades began hemorrhaging cash in the twenty-first century. Many went out of business, and many others lost most of their value. In the 1990s the *New York Times* bought the *Boston Globe* for $1.1 billion and the *Worcester Telegram &*

Gazette for $295 million. In 2013 the *New York Times* sold both newspapers to Boston Red Sox owner John W. Henry for $70 million, or 95 percent less than it had paid for them [82]. Two Philadelphia newspapers lost about 90 percent of their sales value between 2006 and 2012 [82].

The weakening of newspapers is likely to continue. Newspapers continue to get about 20 percent of advertising revenue, even though they account for only about 5 percent of the time Americans spend on media. There is a good chance advertisers will continue to shift their spending away from print media to ads placed on mobile devices [83].

Are newspapers necessary to the healthy functioning of a democracy? The Founding Fathers of the United States were firm believers in the role newspapers could play in ensuring an informed citizenry and holding the powerful to account. Thomas Jefferson wrote, "[W]ere it left to me to decide whether we should have a government without newspapers or newspapers without a government, I should not hesitate a moment to prefer the latter" [84]. The power of the press, often called the Fourth Estate, was demonstrated repeatedly in twentieth-century America. Here are three illustrative examples. In the early 1900s investigative journalist Ida Tarbell's exposé of John D. Rockefeller and the Standard Oil

Company helped lead to the determination that Standard Oil was violating antitrust laws and the subsequent breakup of the company. In 1971 the *New York Times* published the Pentagon Papers, revealing a wealth of information about the conduct of the Vietnam War during the Kennedy and Johnson administrations that had been kept secret from the American public. Bob Woodward and Carl Bernstein's investigation of the White House's involvement in the break-in of the Democratic National Headquarters at the Watergate Hotel in 1972 led to the resignation of President Richard Nixon in 1974.

To be fair, there is plenty of evidence that Americans' interest in newspapers was ebbing well before the creation of Craigslist and the start of the online advertising revolution. Newspaper circulation per capita has been steadily declining since the late 1940s [85]. However, until the turn of the century the best newspapers continued to make healthy profits by introducing automation to make producing and printing newspapers less labor-intensive, consolidating with other newspapers (reducing competition), and steadily increasing their advertising rates. What has proven to be a much more difficult challenge for newspapers to overcome has been devising a strategy to remain profitable in an environment of steadily declining advertising revenues.

Are print newspapers facing extinction in the United States? If so, can the Fourth Estate retain its vibrancy, power, and independence without traditional newspapers?

3.7 Censorship

Censorship is the attempt to suppress or regulate public access to material considered offensive or harmful. Historically, most censorship has been exercised by governments and religious institutions. For example, Roman censors banished the poets Ovid and Juvenal for their writings. During the Middle Ages the Inquisition suppressed the publication of many books, including the work of Galileo Galilei.

Censorship became a much more complicated issue with the invention of the printing press. The printing press broke the virtual monopoly held by governments and religious institutions on distributing material to a large audience, and the increase in printed material resulted in a greater number of literate people. For the first time, private individuals could broadcast their ideas to others on a wide scale.

In many countries, religious institutions continue to play a significant role in determining what material should be accessible to the public. In Western democracies, the gradual separation of church and state has left the government as the sole institution responsible for censorship.

3.7.1 Direct Censorship

Direct censorship has three forms: government monopolization, prepublication review, and licensing and registration.

The first form of direct censorship is government monopolization. In the former Soviet Union, for example, the government owned all the television stations, radio stations, and newspapers. Private organizations could not even own a photocopy machine. Government monopolization is an effective way to suppress the flow of information. Modern computer and communication technology makes government monopolization much more difficult than in the past.

Prepublication review is the second form of direct censorship. This form of censorship is essential for material the government wishes to keep secret, such as information about its nuclear weapons program. Most governments have laws restricting the publication of information that would harm national security. In addition, autocratic governments typically block publication of material deemed injurious to the reputations of their rulers.

The third form of direct censorship is licensing and registration. This form of censorship is typically used to control media with limited bandwidth. For example, only a limited number of radio and television stations can be accommodated on the electromagnetic spectrum. Hence a radio or television station must obtain a license to broadcast at a particular frequency. Licensing invites censorship. For example, the US Federal Communications Commission has banned the use of certain four-letter words. This led to a challenge that went all the way to the US Supreme Court, as we see in Section 3.8.3.

3.7.2 Self-Censorship

Perhaps the most common form of censorship is self-censorship: a group deciding for itself not to publish material. In some countries a publisher may censor itself in order to avoid persecution. For example, after US-led forces toppled the regime of Saddam Hussein in April 2003, CNN's chief news executive, Eason Jordan, admitted that CNN had suppressed negative information about the actions of the Iraqi government for more than a decade in order to keep CNN's Baghdad bureau open and protect Iraqi employees of CNN [86].

In other countries, publishers may want to maintain good relations with government officials. Publications compete with each other for access to information. Often this information is available only from government sources. Publishers know that if they offend the government, their reporters may not be given access to as much information as reporters for rival publications, putting them at a competitive disadvantage. This knowledge can lead a "free" press to censor itself.

Publishers have adopted ratings systems as a way of helping people decide if they (or their children) should access particular offerings. For example, television stations in the United States broadcast shows with "mature content" late in the evening. Voluntary ratings systems help people decide if they (or their children) will see a movie, watch a television show, or listen to a CD.

The Web does not have a universally accepted ratings system. Some Web sites practice a form of labeling. For example, the home page may warn the user that the site contains nudity and require the user to click on an "I agree" button to enter the site. However, other sites have no such warnings. People who stumble onto these sites are immediately confronted with images and text they may find offensive.

3.7.3 Challenges Posed by the Internet

Five characteristics of the Internet make censorship more difficult:

1. *Unlike traditional one-to-many broadcast media, the Internet supports many-to-many communications*.

   While it is relatively easy for a government to shut down a newspaper or a radio station, it is more difficult for a government to prevent an idea from being published on the Internet, where millions of people have the ability to post Web pages.

2. *The Internet is dynamic*.

   Millions of new devices are being connected to the Internet each year.

3. *The Internet is huge*.

   There is simply no way a team of human censors can keep track of *everything* that is posted on the Web. While automated tools are available, they are fallible. Hence any attempt to control access to material stored on the Internet cannot be 100 percent effective.

4. *The Internet is global.*

   National governments have limited authority to restrict activities happening outside their borders.

5. *It is hard to distinguish between children and adults on the Internet.*

   How can an "adult" Web site verify the age of someone attempting to enter the site?

3.7.4 Government Filtering and Surveillance of Internet Content

Despite the difficulties facing those who would seek to censor Internet content, studies reveal that governments around the globe are in fact limiting access to the Internet in a variety of ways [87].

One approach is to make the Internet virtually inaccessible. In North Korea, for example, only about 20,000 people have access to the Internet, representing 0.1% of the population [88].

In other countries, Internet access is easier but still carefully controlled. For example, the Internet backbone in Saudi Arabia is owned by the government, and all Internet traffic to and from the rest of the world flows through two gateways, which block pornography sites, gambling sites, and many other pages deemed to be offensive to Islam or the government of Saudi Arabia [**89**].

The Chinese government has blocked access to the Internet during times of social unrest. For example, in July 2009, China responded to ethnic riots in the autonomous region of Xinjiang by turning off Internet service to the entire region for 10 months [**90**, **91**].

In addition, China has built one of the world's most sophisticated Web filtering systems [**92**]. The Great Firewall of China prevents Chinese citizens from accessing certain Internet content by blocking messages coming from blocklisted sites, which include Google, YouTube, and Facebook [**93**]. According to Freedom House, the Chinese Communist Party's Central Propaganda Department employs "hundreds of thousands or even millions of people to monitor, censor, and manipulate online content" [**93**]. The government shuts down Web sites and censors blogs that criticize government policy, discuss politically sensitive

topics, or provide information that puts the government in a bad light. Among the Web sites blocklisted by the government include those containing pornography, those associated with the Dalai Lama or the Falun Gong, those referring to the 1989 military crackdown, and those run by certain news organizations, such as Voice of America and BBC News. Before the 2008 Summer Olympics, the International Olympic Committee assured journalists that they would have unfettered access to the Internet during their stay in Beijing, but once the journalists arrived in Beijing, they discovered that many sites were blocked. The International Olympic Committee admitted that it had agreed to allow the Chinese government to block sensitive sites "not considered Games related" [**94**]. The Chinese government is also trying to find ways to regulate access to virtual private networks, which many Chinese people use to circumvent the Great Firewall [**93**].

Meanwhile, Western nations have different standards about what is acceptable and what is not. For example, Germany forbids access to any neo-Nazi Web site, but Web surfers in the United States can access many such sites.

Political satire and pornography are easily available through American ISPs. Americans are used to political satire, but

many citizens are concerned about the corrupting influence of pornography, particularly on minors. Since 1996 the US Congress has passed three laws aimed at restricting children's access to sexually explicit material on the Web: the Communications Decency Act, the Child Online Protection Act, and the Children's Internet Protection Act. The first two laws were ruled unconstitutional by the US Supreme Court; the third was upheld by the Supreme Court in June 2003.

3.7.5 Ethical Perspectives on Censorship

It is interesting that Immanuel Kant and John Stuart Mill, who had quite different ethical theories, had similar views regarding censorship.

Kant's Views on Censorship

As a thinker in the tradition of the Enlightenment, Kant's motto was, "Have courage to use your own reason" [95]. Kant asks the rhetorical question, "Why don't people think for themselves?" and answers it: "Laziness and cowardice are the reasons why so great a portion of mankind, after nature has long since discharged them from external direction, nevertheless remain under lifelong tutelage, and why it is so

easy for others to set themselves up as their guardians. It is so easy not to be of age. If I have a book which understands for me, a pastor who has a conscience for me, a physician who decides my diet, and so forth, I need not trouble myself. I need not think, if I can only pay—others will readily undertake the irksome work for me" [**95**, p. 85].

The Enlightenment was a reaction to the institutional control over thought held by the aristocracy and the Church. Kant believed he was living in a time in which the obstacles preventing people from exercising their own reason were being removed. He opposed censorship as a backward step.

Mill's Views on Censorship

John Stuart Mill also championed freedom of expression. He gave four reasons why freedom of opinion, and freedom of expression of opinion, were necessary.

First, none of us is infallible. All of us are capable of error. If we prevent someone from voicing their opinion, we may actually be silencing the voice of truth.

Second, while the opinion expressed by someone may be erroneous, it may yet contain a kernel of truth. In general, the

majority opinion is not the whole truth. We ought to let all opinions be voiced so that all parts of the truth are heard.

Third, even if the majority opinion should happen to be the whole truth, it is in the clash of ideas that this truth is rationally tested and validated. The whole truth left untested is simply a prejudice.

Fourth, an opinion that has been tested in the fire of a free and open discourse is more likely to have a "vital effect on the character and conduct" [**96**, p. 61].

Therefore, Mill, like Kant, fundamentally supported the free exchange of ideas, with the conviction that good ideas would prevail over bad ones. Applying their philosophy to the World Wide Web, it seems they would support the free exchange of opinions and oppose any kind of government censorship of opinions.

Mill's Principle of Harm

However, a lack of government censorship can also lead to harm. Under what circumstances should the government intervene? Mill proposed the principle of harm as a way of deciding when an institution should intervene in the conduct of an individual.

Principle of Harm

> The only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant [**96**, p. 12].

In other words, the government should not get involved in the private activities of individuals, even if the individuals are doing something to harm themselves. Only if individuals' activities are harming other people should the government step in.

The principle of harm can be used to explain the position of most Western democratic governments with respect to censoring pornographic material depicting adults. Some ethicists conclude it is not wrong for adults to view pornography depicting adults. Others hold that this activity is immoral. If the activity is immoral, it is more certain the harm is being done to the individual consumer; less certain is

how much harm is being done to other people. Hence the principle of harm can be used as an argument why the government should not be trying to prevent adults from using pornography depicting adults.

3.8 Freedom of Expression

In the United States, freedom of expression is one of the most cherished—and most controversial—rights. In this section we explain the history behind the adoption of the First Amendment to the United States Constitution. We also explore why the freedom of expression has not been treated as an absolute right.

3.8.1 History

At the time of the American Revolution, any criticism of government was seen as a threat to public order and could result in fines and/or imprisonment. Restrictions on freedom of speech in England date back to 1275 and a law called De Scandalis Magnatum. According to this law, a person could be imprisoned for spreading stories about the King that could have the effect of weakening the loyalty of his subjects. The scope of the law became much broader through numerous revisions over the next two centuries. Eventually, it

encompassed seditious words and words spoken against a wide variety of government officials, including justices [97].

De Scandalis Magnatum was administered by the Court of Star Chamber, or "Star Chamber" for short. The Star Chamber reported directly to the King, and it did not have to obey traditional rules of evidence. Rulings of the Star Chamber demonstrated that a person could be convicted for making a verbal insult or for something written in a private letter. The Star Chamber was abolished in 1641, but the law continued to be enforced through Common Law courts [97].

At the end of the eighteenth century, freedom of the press in England and its colonies meant freedom to print without a license. In other words, there were no **prior restraints** on publication. People could publish what they pleased. However, those who published material found to be seditious or libelous would face severe consequences [97].

The law against libel simply considered if the material printed was harmful; arguing that the information was true was not relevant to the proceedings and could not be used in a publisher's defense. Between 1760 and the end of the American Revolution, about 50 people were successfully prosecuted for libel. To prevent such prosecutions from

continuing, most states adopted bills of rights after gaining independence from England [97].

In May 1787, delegates from the thirteen states gathered in Philadelphia to revise the Articles of Confederation. Soon they were drafting a completely new Constitution. Delegate George Mason, author of the Virginia Declaration of Rights, strongly opposed the proposed Constitution because it contained no declaration of the rights of the citizens. Patrick Henry and other political leaders shared Mason's objections [97].

While the proposed Constitution was ratified by all thirteen states, most state legislatures adopted the Constitution with the expectation that Congress would offer amendments addressing the human-rights concerns brought up by the opponents of the Constitution. During the first Congress, James Madison proposed 12 such amendments. All 12 of these amendments were sent to the states for ratification. Of these 12 amendments, 10 were quickly ratified. Today these 10 amendments are commonly known as the Bill of Rights. The first of these amendments, the one Madison considered most essential, was the one guaranteeing freedom of speech and freedom of the press [97].

First Amendment to the United States Constitution

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

3.8.2 Freedom of Expression Not an Absolute Right

The primary purpose of the First Amendment's free speech guarantee is political. Free speech allows an open discussion of public issues. It helps make government responsive to the will of the people [98].

However, the First-Amendment right to free expression is not limited to political speech. Nonpolitical speech is also covered. There are good reasons for protecting nonpolitical as well as political speech. First, it is sometimes hard to draw the line between the two. Asking a judge to make the distinction turns it into a political decision. Second, society can benefit from nonpolitical as well as political speech. Hence the free-speech guarantee of the First Amendment also promotes scientific and artistic expression. For the same reason, the definition of "speech" encompasses more than words. Protected "speech" includes art and certain kinds of conduct, such as burning a US flag [**99**].

Decisions by the US Supreme Court have made clear that freedom of expression is not an absolute right. Those who abuse this freedom and harm the public may be punished. For example, protection is not given to "libel, reckless or calculated lies, slander, misrepresentation, perjury, false advertising, obscenity and profanity, solicitation of crime, and personal abuse or 'fighting' words," because these actions do not serve the ends of the First Amendment [**98**].

Various restrictions on freedom of speech are justified because of the greater public good that results. For example, US law prohibits cigarette advertising on television because

cigarette smoking has detrimental effects on public health. Some cities use zoning laws to concentrate adult bookstores in a single part of town because the presence of adult bookstores lowers property values and increases crime.

3.8.3 FCC v. Pacifica Foundation

To illustrate limits to First Amendment protections, we consider the decision of the US Supreme Court in the case of *Federal Communications Commission v. Pacifica Foundation et al.*

In 1973 George Carlin recorded a performance made in front of a live audience in California. One track on the resulting record is a 12-minute monologue called "Filthy Words." In the monologue Carlin lists seven words that "you couldn't say on the public, ah, airwaves, um, the ones you definitely wouldn't say, ever" [100]. The audience laughs as Carlin spends the rest of the monologue creating colloquialisms from the list of banned words.

On the afternoon of October 30, 1973, counterculture radio station WBAI in New York aired "Filthy Words" after warning listeners the monologue contained "sensitive

language which might be regarded as offensive to some" [**101**]. A few weeks after the broadcast, the Federal Communications Commission (FCC) received a complaint from a man who had heard the broadcast on his car radio in the presence of his son. In response to this complaint, the FCC issued a declaratory order and informed Pacifica Foundation (the operator of WBAI) that the order would be placed in the station's license file. The FCC warned Pacifica Foundation that further complaints could lead to sanctions.

Pacifica sued the FCC, and the resulting legal battle reached the US Supreme Court. In 1978 the Supreme Court ruled, in a 5–4 decision, that the FCC did not violate the First Amendment [**101**]. The majority opinion states, "Of all forms of communication, it is broadcasting that has received the most limited First Amendment protection." There are two reasons why broadcasters have less protection than booksellers or theater owners:

1. "*Broadcast media have a uniquely pervasive presence in the lives of all Americans.*" [**101**]

   Offensive, indecent material is broadcast into the privacy of citizens' homes. Since people can change stations or turn their radios on or off at any time, prior warnings cannot completely protect people from being

exposed to offensive material. While someone may turn off the radio after hearing something indecent, that does not undo a harm that has already occurred.

2. *"Broadcasting is uniquely accessible to children, even those too young to read."* [**101**]

   In contrast, restricting children's access to offensive or indecent material is possible in bookstores and movie theaters.

The majority emphasized that its ruling was a narrow one and that the context of the broadcast was all-important. The time of day at which the broadcast occurred (2 p.m.) was an important consideration, because that affected the composition of the listening audience.

3.8.4 Case Study: Leah's Blog

Leah is a journalism major who maintains a popular blog focusing on campus life. Leah attends a private birthday party in someone's apartment for her friend Jamal, a college student active in the Whig Party on campus. Someone gives Jamal a Tory Party T-shirt as a gag gift, and Jamal puts it on. Leah uses her cell phone to get a picture of Jamal wearing the

T-shirt when he is looking the other way. Jamal gives Leah a ride home after the party, but she does not tell him about the photo. When she is back in her apartment, she posts the photo on her blog. In the blog she identifies Jamal and explains the context in which the photo was taken.

The story is read by many people both on and off campus. The next day Jamal confronts Leah, yells at her for posting the photo, and demands that she remove it from her Web site. Leah complies with Jamal's request by removing the photo, and the two of them remain friends. As a result of the incident, Jamal becomes more popular on campus, and the number of people who read Leah's blog increases.

)

Was it wrong for Leah to post the picture of Jamal on her blog without first getting his permission?

Kantian Analysis

By uploading Jamal's photo to her blog without first asking his permission, Leah didn't respect Jamal's autonomy. Instead, she treated him as a means to her end of increasing the readership of her blog. Therefore, her action was wrong according to the second formulation of the Categorical Imperative.

Social-Contract-Theory Analysis

The birthday party was held in the apartment of one of Jamal's friends. In this private setting and among friends, Jamal had a legitimate expectation that what happened during the party would not be broadcast to the world. By secretly taking a photo of Jamal doing something out of character and posting that photo on her blog, Leah violated Jamal's right to privacy. For this reason Leah's action was wrong.

Act-Utilitarian Analysis

We need to determine the positive and negative consequences of Leah's action on the two people involved. Leah increased the popularity of her blog, which is precisely the positive outcome she wanted (+10). Jamal's anger at Leah shows that he was hurt and upset by what she did, but after he confronted her, she removed the photo from her Web site and they reconciled. Therefore, while the intensity of this negative consequence to Jamal was significant, its duration was brief (−5). As a result of the posting, Jamal became more popular on campus, a very good thing for someone active in campus politics (+10). Jamal had Leah to thank for this boost in his popularity, further quenching the unhappiness he initially felt when he learned what she had done (+2). We

conclude that the short-term consequences for both Leah and Jamal were positive (totaling +17).

The long-term consequences are difficult to determine. It is possible that the photo could land in the wrong hands and be used to discredit Jamal someday in the future (−100), but this would depend on many factors. Jamal is currently politically active. Is he going to stay active in Whig politics after he graduates from college (50 percent)? The photo was only on the Web for a day. Did anyone download it (20 percent)? If so, what is the chance that someday the photo will fall into the hands of someone who wants to make Jamal look bad (10 percent)?

An important part of a utilitarian analysis is looking at the certainty of each consequence: in other words, the probability that it will happen. The short-term consequences of Leah's action are certainly positive for both Leah and Jamal ($+17 \times 100\% = +17$). The long-term negative consequences, if any, are not certain at all ($-100 \times 50\% \times 20\% \times 10\% = -1$). Adding the calculated short-term benefits (+17) to the calculated long-term harms (−1) yields a total benefit of 16, and we conclude her action had a good outcome.

Rule-Utilitarian Analysis

Let's consider what would happen if everyone were constantly taking photos of everyone they bumped into and posting them on the Web. There would be some positive consequences. It would be easier for people to see what their friends were up to. People might be more reluctant to engage in illegal activities if they thought photo or video evidence might appear on the Web. There would also be a variety of negative consequences. Once people started to feel as if they were always being photographed, they would become self-conscious, making it more difficult for them to simply be themselves. People would be less free to take off their public persona and express their true feelings. Inevitably, people would post photos that caused hard feelings and led to strained relationships. Ultimately, the negative consequences seem to be more weighty than the positive consequences, and we conclude Leah's action was wrong.

Virtue-Ethics Analysis

Leah and Jamal are friends. Aristotle recognized that people are social beings and that friendship plays an important role in *eudaimonia*, or human flourishing. True friends trust each other and seek each other's good. Reciprocity and an equality of interest are fundamental elements of friendship. There was no reciprocity when Leah sneakily took Jamal's photo

without his knowledge; she exploited him by taking something from him without giving him anything in return. She did not act as a friend when she put her own interest above that of Jamal. After the party, Leah had another opportunity to be honest with Jamal. Unfortunately, she did not trust Jamal enough to admit she had taken the picture and ask his permission before posting the photo. Instead, she said nothing to Jamal and simply posted the photo to her blog. Overall, Leah's actions at several points in the story do not seem to be characteristic of a good friend.

Summary

The analyses from the perspectives of Kantianism, social contract theory, rule utilitarianism, and virtue ethics do not support Leah posting the photo without asking Jamal's permission, though each analysis uses a different line of reasoning to reach that conclusion. Leah imagined (correctly, as it turns out) that Jamal would be angry if she took a photo of him wearing the Tory Party T-shirt, and that is why she took the photo when he wasn't looking. Leah figured it would be better to beg for forgiveness than ask for permission, but what she did was cut Jamal out of a decision that affected both of them. This is no way to treat anybody, much less a friend. Leah would have been better off trying to

persuade Jamal that putting the photo on her blog would be to their mutual advantage, posting the image only after obtaining his consent.

3.9 Children and Inappropriate Content

Many parents and guardians believe they ought to protect their children from exposure to pornographic and violent materials. A few years ago the center of concern was the Web, and a large software industry sprang up to provide browsers with the ability to block inappropriate images. Now smartphones are ubiquitous, and some caregivers are being forced to confront the unpleasant reality that children have texted unclothed or sexually explicit images of themselves to friends or even strangers.

3.9.1 Web Filters

A **Web filter** is a piece of software that prevents certain Web pages from being displayed by your browser. While you are running your browser, the filter runs as a background process, checking every page your browser attempts to load.

If the filter determines that the page is objectionable, it prevents the browser from displaying it.

Filters can be installed on individual computers, or an ISP may provide filtering services for its customers. Programs designed to be installed on individual computers, such as CyberSentinel and Spector Pro, can be set up to email caregivers as soon as they detect an inappropriate Web page [102].

Typical filters use two different methods to determine if a page should be blocked. The first method is to check the URL of the page against a blocklist of objectionable sites. If the Web page comes from a blocklisted site, it is not displayed. The second method is to look for combinations of letters or words that may indicate a site has objectionable content.

Neither of these methods is foolproof. The Web contains millions of pages containing pornography, and new sites continue to be created at a high rate, so any blocklist of pornographic sites will be incomplete by definition. Some filters sponsored by conservative groups have blocklisted sites associated with liberal political causes, such as those sponsored by the National Organization for Women and LGBTQIA+ groups. The algorithms used to identify

objectionable words and phrases can cause Web filters to block out legitimate Web pages.

3.9.2 Child Internet Protection Act

In March 2003, the Supreme Court weighed testimony in the case of *United States v. American Library Association*. The question: Can the government require libraries to install antipornography filters in return for receiving federal funds for Internet access?

More than 14 million people access the Internet through public library computers. About one-sixth of the libraries in the United States have already installed filtering software on at least some of their computers. The Child Internet Protection Act requires that libraries receiving federal funds to provide Internet access to its patrons must prevent children from getting access to visual depictions of obscenity and child pornography. The law allows adults who desire access to a blocked page to ask a librarian to remove the filter.

In his testimony before the Supreme Court, Solicitor General Theodore Olson argued that since libraries don't offer

patrons X-rated magazines or movies, they should not be obliged to give them access to pornography over the Internet.

Paul Smith, representing the American Library Association and the American Civil Liberties Union, argued that in their attempt to screen out pornography, filters block tens of thousands of inoffensive pages. He added that requiring adults to leave the workstation, find a librarian, and ask for the filter to be turned off would be disruptive to their research and would stigmatize them.

In June 2003, the US Supreme Court upheld CIPA, ruling 6–3 that antipornography filters do not violate First-Amendment guarantees [**103**]. Chief Justice William Rehnquist wrote, "A public library does not acquire Internet terminals in order to create a public forum for Web publishers to express themselves, any more than it collects books in order to provide a public forum for the authors of books to speak . . . Most libraries already exclude pornography from their print collections because they deem it inappropriate for inclusion" [**104**].

3.9.3 Ethical Evaluations of CIPA

In this section we evaluate CIPA from the perspectives of Kantianism, act utilitarianism, and social contract theory.

Kantian Evaluation

We have already covered Kant's philosophical position against censorship. He believed that allowing people to use their own reason would lead to society's gradual enlightenment. In this case, however, the focus is narrower. Rather than talking about censorship in general, let's look at CIPA in particular.

The goal of CIPA is to protect children from the harm caused by exposure to pornography. The way the goal is being implemented is through Web filters. Studies have demonstrated that Web filters do not block all pornographic material but do block some nonpornographic Web pages. Some nonpornographic information posted on the Web is not easily accessible at libraries implementing government-mandated Web filters. The people posting this information did not consent to their ideas being blocked. Hence the decision to require the use of Web filters treats the creators of nonoffensive but blocked Web pages solely as means to the end of restricting children's access to pornographic materials. This analysis leads us to conclude that CIPA is wrong.

Act-Utilitarian Evaluation

Our second evaluation of CIPA is from an act-utilitarian point of view. What are the consequences of passing CIPA?

1. While not all children access the Web in public libraries, and while Web filtering software is imperfect, it is probable that enacting CIPA results in fewer children being exposed to pornography, which is good.
2. Because Web filters are imperfect, people are unable to access some legitimate Web sites. As a result, Web browsers in libraries are less useful as research tools, a harmful consequence.
3. Adult patrons who ask for filters to be removed may be stigmatized (rightly or not) as people who want to view pornography, a harm to them.
4. Some blocked sites may be associated with minority political views, reducing freedom of thought and expression, which is harmful.

Whenever we perform the utilitarian calculus and find some benefits and some harms, we must decide how to weigh them. This is a good time to think about utilitarian philosopher Jeremy Bentham's seven attributes. In particular,

how many people are in each affected group? What is the probability the good or bad event will actually happen? How soon is the event likely to occur? How intense will the experience be? To what extent is the pain not diluted by pleasure or vice versa? How long will it last? How likely is the experience to lead to a similar experience? Actually performing the calculus for CIPA is up to each person's judgment. Different people could reach opposite conclusions about whether enacting CIPA is the right thing for the US government to do.

Social-Contract-Theory Evaluation

In social contract theory, morally binding rules are those rules mutually agreed to in order to allow social living [**105**]. Freedom of thought and expression is prized. According to John Rawls, "liberty of conscience is to be limited only when there is a reasonable expectation that not doing so will damage the public order which the government should maintain" [**106**].

It would be difficult to gain consensus around the idea that the private viewing of pornography makes social living no longer possible. For this reason, the private use of pornography is considered to be outside the social contract and nobody else's business. However, when we think about

the availability of pornography in public libraries, the issue gets thornier.

Some argue that allowing people to view pornography in a public place demeans women, denying them dignity as equal persons [**107**]. On the other hand, we know that filtering software is imperfect. In the past, it has been used to promote a conservative political agenda by blocking sites associated with other viewpoints [**108, 109**]. Hence it reduces the free exchange of ideas, limiting the freedoms of thought and expression. For some adults, public libraries represent their only opportunity to access the Web at no cost. In order to be treated as free and equal citizens, they should have the same Web access as people who have Internet access from their homes. If Web filters are in place, their access is not equal because they must ask for permission to have the filters disabled. Finally, while most people would agree that children should not be exposed to pornographic material, it would be harder to convince reasonable people that social living would no longer be possible if children happened to see pornography in a library.

Our analysis from the point of view of social contract theory has produced arguments both supporting and opposing the Children's Internet Protection Act. However, installing filters

does not seem to be necessary to preserve the public order. For this reason, the issue is outside the social contract and freedom of conscience should be given precedence.

3.9.4 Sexting

Sexting refers to sending sexually suggestive text messages or emails containing nude or nearly nude photographs [**110**]. Sexting has drawn a lot of media attention, but early reports on this phenomenon may have overstated the rates at which teenagers are sexting. More recent surveys indicate that between 3 and 7 percent of teens are sexting, and only 1 percent of teens have actually sent photos showing intimate areas of their bodies [**111**].

Whatever its frequency, sexting has had a serious impact on some people's lives. Here are three incidents.

Ohio high-school student Jesse Logan sent nude pictures of herself to her boyfriend. When they broke up, the ex-boyfriend distributed the photos to other girls in her high school. Jesse endured months of harassment from her high-school classmates and began skipping classes on a daily basis. After attending the funeral of another classmate who died by suicide, Jesse went home and ended her own life [**112**].

Ting- Yi Oei, a 59-year-old assistant principal at Freedom High School in South Riding, Virgina, was asked to investigate rumors that students were distributing nude photographs on their cell phones. His investigation led to a 16-year-old boy, who had a photo of a 17-year-old girl on his phone. In the photo, the girl was posing in her panties, with her arms mostly covering her breasts. Oei showed the image to the principal, who told him to keep a copy on his computer as evidence. Two weeks later the same boy got in trouble again, and Oei suspended him for two weeks. When Oei met with the boy's mother, he told her about the earlier photo incident. The boy's mother was upset that Oei hadn't immediately told her about the photo, and she demanded that Oei revoke her son's suspension. When Oei refused, the mother went to the police and told them about the photo. Sheriff's investigators came to the school and found the photo of the girl on Oei's computer. County prosecutor James Plowman gave Oei an ultimatum: resign or face felony charges for possession of child pornography. Plowman's assistant told the press, "We just feel very strongly that this is not someone who should be in the Loudoun County school system." Oei refused to resign, and in August 2008, a grand jury indicted him for possession of child pornography. The school district removed him from his position as vice

principal and reassigned him to a job at a testing center. Oei had to take out a second mortgage on his house to pay legal expenses. In April 2009, Loudoun Circuit Court Judge Thomas Horne dismissed the charges, noting that nudity alone is not sufficient to categorize an image of a minor as child pornography. Though never convicted, Oei ended up deeply in debt and with a tarnished reputation, unsure if he would ever return to his former position at the high school [**113**].

After Phillip Alpert got into an argument with his 16-year-old girlfriend, he emailed a nude photo of her to dozens of her friends and family members. The Orlando, Florida, police arrested Alpert, who had just turned 18, charging him with sending child pornography, a felony. Alpert was sentenced to five years' probation and required to register with the state of Florida as a sex offender. He will remain a registered sex offender until he is 43 years old [**114**].

There appears to be a widespread sentiment that child pornography laws should not be used to prosecute teenagers who are caught sexting. As of August 2022, 13 states in the United States had passed laws allowing minors who sext to be diverted outside the formal justice system [**115**].

3.10 Breaking Trust

Some people use the Internet for purposes of identity theft or sexual assault. Companies and individuals have used fake online reviews to drum up business. Many people have been humiliated by the widespread dissemination of photos or videos they expected to be kept private.

3.10.1 Identity Theft

Dorothy Denning defines **identity theft** as "the misuse of another person's identity, such as name, Social Security number, driver's license, credit card numbers, and bank account numbers. The objective is to take actions permitted to the owner of the identity, such as withdraw funds, transfer money, charge purchases, get access to information, or issue documents and letters under the victim's identity" [**116**].

By far the leading form of identity theft in the United States involves the fraudulent use of an existing credit card account or bank account. In 2017 about 7 percent of adults in the United States reported being the victims of identity fraud [**117**]. Fortunately, US law says that a consumer's liability for losses due to credit card fraud are limited to $50 if reported

promptly. Most victims end up paying nothing out of pocket because their banks and credit card companies offer zero-liability fraud protection.

Point- of-sale fraud has declined rapidly with the adoption of EMV (embedded chip) credit cards and terminals. Identify fraud is increasingly happening online, where it is more difficult for merchants to verify that transactions are being authorized by the rightful cardholders because the cardholders cannot present their cards for inspection. So-called "card-not-present fraud" is now 81 percent more likely than point-of-sale fraud [**117**].

Identity thieves are much more likely to use low-tech methods rather than sophisticated online attacks to gain access to the account information they need. A 2008 survey of identity theft victims revealed that in 43 percent of the cases, the theft was the result of a lost or stolen wallet, credit card, checkbook, or another physical document [**118**]. Some identity thieves engage in **dumpster diving—** looking for personal information in garbage cans or recycling bins. Old bills, bank statements, and credit card statements contain a wealth of personal information, including names, addresses, and account numbers. Another simple way to get information

is through **shoulder surfing**—looking over the shoulders of people filling out forms.

Gathering financial information via spam is called **phishing** (pronounced "fishing"). Thieves send out spam messages designed to look as if they originated from PayPal, eBay, or another well-known Internet-active business. Through these messages they hope to con unsuspecting recipients into connecting with authentic-looking Web sites and revealing their credit card numbers or other personal information. For example, a victim might receive an email message purportedly from PayPal, asking the person to go to the PayPal Web site to confirm a transaction. The email message contains a hypertext link. When the person clicks on the link, they are connected to the counterfeit PayPal site.

College students are five times more likely to be victims of identity theft than average adults, for a variety of reasons. They use a lot of digital devices, and many do not secure them properly with strong passwords. They tend to post a lot of personal information on social media sites. College students are particularly vulnerable to low-tech methods of identity theft. A high percentage of them live in close quarters with others, and some do not take care to secure sensitive information. Dorm rooms are often left wide open, with

checkbooks and financial documents kept in unlocked desk drawers. Students may throw documents containing personal financial information into the trash, where they can be retrieved by dumpster divers [**119**].

The Identity Theft and Assumption Act of 1998 makes identity theft a federal crime. In 2004 Congress passed the Identity Theft Penalty Enhancement Act, which lengthened prison sentences for identity thieves [**120**]. A variety of law-enforcement agencies investigate alleged violations of this law: the US Secret Service, the FBI, the US Postal Inspection Service, and the Office of the Inspector General of the Social Security Administration.

3.10.2 Fake Reviews

A 2014 survey of North Americans by BrightLocal revealed that 88 percent had used online reviews in the past 12 months to gauge the quality of a local business, and 39 percent read reviews regularly. Restaurants, hotels, doctors and dentists, and beauty salons were the business types most frequently searched by consumers [**121**].

About three-quarters of consumers (72 percent) told surveyers that “positive reviews make them trust a local business more” [**121**]. Unfortunately, a significant percentage

of online reviews are fraudulent. Some businesses try to boost sales by posting fake positive reviews of their enterprises or fake negative reviews of their competitors. Alternatively, they may hire third parties to do these things.

One study estimated that 16 percent of restaurant reviews on Yelp were fraudulent [**122**]. Another researcher concluded that one-third of all Internet reviews were fake [**122**]. Fake reviews undermine the credibility of the information consumers are using to make purchasing decisions.

In some instances consumers can identify suspect reviews. For example, by tracing through the reviewer's alias, a consumer can see how many reviews that reviewer has written. An alias that has posted only a single review is suspicious [**122**]. Another way to screen reviews is to look at the number of stars. "Pretty much all fake reviews are 5-star or 1-star reviews. Nobody leaves a fake 3-star review. What would be the point?" says Nicholas White of the *Daily Dot* [**123**].

Online review provider Yelp invests millions of dollars annually attempting to identify fake reviews posted to its site. About 10 percent of its employees are on the hunt for fraudulent reviews, and it has also developed sophisticated software to detect suspicious reviews. About 25 percent of

the reviews submitted to Yelp don't make it past the screening and are not recommended [**123**].

3.10.3 Online Predators

Instant messaging refers to a system allowing two people to "chat" via typing in real time over the Internet. Instant messaging is popular among young adults because it allows them to communicate without paying SMS text-messaging charges. Kik Messenger is a popular instant messaging app for smartphones; as of January 2018, it had 300 million users, including 33 percent of the teens in the United States [**124**]. In addition to text messages, Kik Messenger also allows users to send images and videos.

In August 2013, police began to issue warnings about people using Kit Messenger to facilitate their perpetration of sexual abuse and assault [**125**]. A few months later, 39-year-old Manuel Salto pleaded guilty to third-degree criminal sexual conduct after using Kik Messenger to meet a 13-year-old girl whom he later lured to his home for sexual relations [**126**].

Other apps as well have been used by people who engage in pedophilia. According to police, Whisper is particularly

dangerous because it allows users to post their location, making it easier for predators to find local targets [**127**].

For more than 15 years, police have launched sting operations to arrest people seeking sex with minors. Sometimes these sting operations have resulted in dozens of arrests. For example, the Osceola County sheriff's department in Florida conducted a one-week-long sting operation in January 2012 that resulted in the arrest of 40 adults, including a professional golfer, a teacher, and a swim coach. Deputies arrested the suspects as they arrived at an undercover house, thinking they were going to have sex with a minor. According to the sheriff's department, before the suspects arrived at the rendezvous, most of them had already sent sexually explicit images to the "children" they were chatting with [**128**]. A similar sting operation in Lincolnton, North Carolina, in May 2015 led to 17 arrests [**129**]. Another sting operation in Galveston, Texas, in June 2015 led to the arrest of 11 men and women hoping to have sex with children [**130**].

In 2014 WTSP-TV aired an exposé critical of the sting operations in Polk County, Florida, alleging that detectives were resorting to more extreme methods to keep up their arrest rates. For example, an officer responds to an ad on an

adult dating site, pretending to be an adult woman, but once an online relationship begins to develop, the detective suggests the man might be interested in having sex with "her" child. Some police tactics have resulted in cases being thrown out of court, with judges making comments such as these:

- "It was the agent who repeatedly steered the conversation back to sexual activity with a minor."
- "The government made a concerted effort to lure him into committing a crime."
- "The law does not tolerate government action to provoke a law-abiding citizen to commit a crime" [131].

3.10.4 Ethical Evaluations of Police Sting Operations

Is it morally right for police detectives to pose as children on the Internet to entrap people who seek to have sex with children?

Utilitarian Analysis

Let's consider the various consequences of such a sting operation. A person allegedly interested in having sex with an underage minor is arrested and charged with attempted child rape. Suppose the person is found guilty and must serve time in prison. The direct effects of the sting operation are the denial of one person's freedom (a harm) and an increase in public safety (a benefit). Since the entire public is safer and only a single person is harmed, this is a net good.

The sting operation also has indirect effects. Publicity about the sting operation may deter other people who seek sex with children. This, too, is a beneficial result. It is harder to gauge how knowledge of sting operations influences innocent citizens. First, it may reduce citizens' trust in the police. Many people believe that if they are doing nothing wrong, they have nothing to fear. Others may become less inclined to provide information to the police when requested. Second, sting operations can affect everyone's online experiences. They demonstrate that people are not always who they claim to be. This knowledge may make people less vulnerable to being taken advantage of, but it may also reduce the amount of trust people have in others. Sting operations prove that supposedly private conversations can actually be made public. If instant messaging conversations lack honesty and privacy, people will be less willing to engage in serious

conversations. As a result, instant messaging loses some of its utility as a communications system. How much weight you give to the various consequences of police sting operations using instant messaging determines whether the net consequences are positive or negative.

Kantian Analysis

A Kantian focuses on the will leading to the action rather than the results of the action. The police are responsible for maintaining public safety. People who engage in pedophilia endanger innocent children. Therefore, it is the duty of police to try to prevent them from accomplishing what they intend to do. The will of the police detective is arrest people who engage in pedophilia. This seems straightforward enough.

If we dig a level deeper, however, we run into trouble. In order to arrest a person who wishes to engage in pedophilia, the police must identify this person. Since a person seeking sex with a child unlikely to confess on the spot if asked a question by a police officer, the police lay a trap. In other words, the will of the police detective is to deceive a person who engages in pedophilia in order to catch them. To a Kantian, lying is wrong, no matter how noble the objective. By collecting evidence of instant-messaging conversations, the police detective also violates the presumed privacy of this

medium. While police officers have a duty to protect the public safety, it is wrong for them to break other moral laws in order to accomplish this purpose. From a Kantian point of view, the sting operation is morally wrong.

Social-Contract-Theory Analysis

An adherent of social contract theory could argue that in order to benefit everyone, there are certain moral rules that people communicating online ought to follow. For example, people ought to be honest, and conversations ought to be kept confidential. By misrepresenting identity and/or intentions, the person engaging in pedophilia has broken a moral rule and ought to be punished. In conducting sting operations, however, police detectives also misrepresent their identities and record everything typed by suspects. The upholders of the law have broken the rules, too. Furthermore, we have the presumption of innocence until proof of guilt. What if the police detective, through miscommunication or bad judgment, actually entraps someone who is not a person who engages in pedophilia? In this case, an innocent person has not broken any rules. They were simply in the wrong place at the wrong time. Yet society, represented by the police detective, did not provide the benefits instant messaging users expect to receive (honest

communications and privacy). In short, there is a conflict between society's need to punish a wrongdoer and its expectation that everyone (including the agents of the government) abide by its moral rules.

Summary of Ethical Analyses

To summarize our ethical evaluation of police sting operations, the actions of the police seem immoral from a Kantian point of view. Evaluations using the other ethical theories do not yield a clear-cut endorsement or condemnation of the stings. While the goals of the police are laudable, they accomplish their goals through deception and by revealing details of conversations thought to be private. Sting operations are more likely to be viewed as morally acceptable by someone who is more focused on the results of an action than the methods used; in other words, a consequentialist.

)

3.10.5 False Information

The Web is a more open communication medium than newspapers, radio stations, or television stations. Individuals or groups whose points of view might never be published in a newspaper or broadcast on a television or radio show may create an attractive Web site. The ease with which people

may get information out via the Web is one of the reasons the Web contains billions of pages. However, the fact that no one has to review a Web page before it is published means the quality of information available on the Web varies widely.

You can find many Web sites devoted to the American manned space program. You can also find many Web sites that argue the Moon landings were a hoax by NASA. Many Web sites describe the Holocaust committed by the Nazis before and during World War II. Other sites falsely claim the Holocaust never happened. A TikTok post claiming that the Titanic never sank attracted more than 11 million views before it was deleted [**132**].

Disputes about commonly held assumptions did not begin with the Web. Some television networks and newspapers are well known for giving a forum to people who question information provided through government agencies. Twice in 2001, the Fox TV network aired a program called "Conspiracy Theory: Did We Land on the Moon?" The program concludes NASA faked the Moon landing in the Nevada desert. Supermarket tabloids are notorious for their provocative, misleading headlines. Experienced consumers take into account the source of the information.

Most people would agree that *60 Minutes* on CBS is a more reliable source of information than the *Conspiracy Theory* series. Similarly, people expect information they find in the *New York Times* to be more reliable than the stories they read in a tabloid.

In traditional publishing, various mechanisms are put in place to improve the quality of the final product. For example, before Addison-Wesley published the first edition of this book, an editor sent draft copies of the manuscript to a dozen reviewers who checked it for errors, omissions, or misleading statements. I revised the manuscript to respond to the reviewers' suggestions. After I submitted a revised manuscript, a copy editor made final changes to improve the readability of the text, and a proofreader corrected typographical errors. Every subsequent edition has benefited from the feedback of experienced and knowledgeable college professors reviewing the proposed changes.

Web pages, on the other hand, can be published without any review. As you're undoubtedly well aware, the quality of Web pages varies dramatically. Fortunately, search engines can help people identify those Web pages that are most relevant and of the highest quality. Let's take a look at how the Google search engine does this.

The Google search engine keeps a database of many billions of Web pages. A software algorithm called PageRank ranks the quality of these pages. PageRank invokes a kind of voting mechanism. If Web page A links to Web page B, then page B gets a vote. However, all votes do not have the same weight. If Web page A is itself getting a lot of votes, then page A's link to page B gives its vote more weight than a link to B from an unpopular page.

When a user makes a query to Google, the search engine first finds the pages that closely match the query. It then considers their quality (as measured by the voting algorithm) to determine how to rank the relevant pages.

3.10.6 Cyberbullying

In November 2002, Ghyslain Raza, a high-school student living in Quebec, Canada, borrowed a videotape and used one of the high school's video cameras to film himself awkwardly swinging a golf ball retriever like a light saber, à la Darth Maul in *Star Wars Episode I*. A few months later, the owner of the videotape discovered the content and shared it with some friends. After one of them digitized the scene and made it available on the Internet, millions of people downloaded the file in the first two weeks [**133**]. Ghyslain

was nicknamed “the Star Wars kid,” endured prolonged harassment from other students, and eventually dropped out of school [**134**]. By 2006 the video had been viewed more than 900 million times [**135**].

Cyberbullying is the use of the Internet or the phone system to inflict psychological harm on another person. Frequently, a group gangs up to cyberbully the victim. Examples of cyberbullying include the following:

- Repeatedly texting or emailing hurtful messages to another person
- Spreading lies about another person
- Tricking someone into revealing highly personal information
- “Outing” or revealing someone’s secrets online
- Posting embarrassing photographs or videos of other people without their consent
- Impersonating someone else online in order to damage that person’s reputation
- Threatening or creating significant fear in another person

Surveys have revealed that cyberbullying is common among teenagers. Cox Communications surveyed 655 American teenagers in 2009, and 19 percent reported that they had been cyberbullied online, via cell phone, or through both media. Ten percent of the teenagers admitted to cyberbullying someone else. When asked why they had cyberbullied someone else, the most common responses were "they deserved it" and "to get back at someone" [**110**].

In some instances cyberbullying has led to the suicide of the victim, as in the case of 13-year-old Megan Meier. According to her mother, "Megan had a lifelong struggle with weight and self-esteem" [**136**]. She had talked about suicide in third grade, and ever since then she had been seeing a therapist [**136**]. Megan's spirits soared when she met a 16-year-old boy named Josh Evans on MySpace. They flirted online for four weeks but never met in person. Then Josh seemed to sour on their relationship. One day he let her know that he didn't know if he wanted to be friends with her anymore. The next day he posted the following [**136, 137**]:

> You are a bad person and everybody hates you.
>
> Have a shitty rest of your life.
>
> The world would be a better place without you.

When Megan angrily responded to this post, others ganged up on her: “Megan Meier is a slut”; “Megan Meier is fat” [**136**]. Later that afternoon, Megan died by suicide in her bedroom.

Eventually, the community learned that “Josh Evans” did not exist. The MySpace account had been created just a couple of houses away from the Meier home by 18-year-old Ashley Grills, 13-year-old Sarah Drew, and Lori Drew, Sarah’s mother. Sarah had a falling out with Megan, and Ashley suggested creating the MySpace account to find out what Megan might be saying about Sarah. Lori Drew had approved the plan. Most of the messages from “Josh” had been written by Sarah or Ashley, but Lori Drew had been aware of what they were doing [**138**].

The county’s district attorney declined to prosecute Lori Drew because there was no Missouri law against cyberbullying [**139**]. The FBI investigated the case, however, and in 2008 federal prosecutors charged Drew with four felony counts under the Computer Fraud and Abuse Act for violating the MySpace terms of service. A jury found her not guilty of these crimes but did convict her of three misdemeanors [**140**]. In 2009 a US district judge overturned these convictions, stating that criminal charges should not

have been brought against Drew for breaking a contract with an Internet service provider [**141**].

In April 2009, the Megan Meier Cyberbullying Prevention Act was introduced in the US House of Representatives. The purpose of the proposed law was to "impose criminal penalties on anyone who transmits in interstate or foreign commerce a communication intended to coerce, intimidate, harass, or cause substantial emotional distress to another person, using electronic means to support severe, repeated, and hostile behavior" [**142**]. Some civil libertarians objected to the proposed legislation, arguing that it would take away free-speech rights guaranteed under the First Amendment to the US Constitution. The law did not win approval by the House of Representatives.

3.10.7 Revenge Porn

The *Collins English Dictionary* defines **revenge porn** to be "a pornographic image or film which is published, posted (e.g., on the Internet), or otherwise circulated without the consent of one or more of the participants, usually with malicious and vindictive intent, such as following a break-up" [**143**]. Revenge porn is a special case of cyberbullying.

The Web site Is Anyone Up?, launched in 2010 by Hunter Moore, quickly became a magnet for revenge porn submissions, significantly raising the visibility of this issue. Moore appeared on the talk show *Anderson*, along with two women whose images had appeared on the site without their permission. When asked by Anderson Cooper whether he felt bad about what he had done "to these two women," Moore replied to the women, "No one . . . made you take these pictures. It's 2011; everything's on the Internet" [**144**]. One of the women responded, "If we're choosing to send them to someone we trust, that doesn't mean we expect them to show up on the Internet" [**144**]. Moore shut down the Web site in April 2012. In February 2015 he pleaded guilty to one count of accessing a protected computer to obtain information for financial gain and one count of aggravated identity theft, and in December 2015 he was sentenced to two-and-a-half years in federal prison [**145**].

Posting revenge porn has been criminalized in Australia, France, Germany, Israel, Italy, Japan, Malta, the Philippines, Singapore, South Africa, South Korea, the United Kingdom, and the United States. In 2011, after Noe Iniguez broke up with his girlfriend, he posted topless photos of her on her employer's Facebook page. Three years later Iniguez became

the first person to be convicted under California's law criminalizing the unauthorized posting of nude images [**146**].

In the first six months of 2015, three corporations took action to protect victims of revenge porn. Reddit announced it was banning the posting of sexually explicit images without the consent of the people in the images [**147**]. Twitter updated its rules to include, "You may not post intimate photos or videos that were taken or distributed without the subject's consent," and it promised to remove links to such content [**148**]. Google announced that it would create an online form enabling victims to request that nude or sexually explicit images of themselves posted without their consent be withheld from Google search results [**149**].

3.11 Internet Addiction

Many people spend a great deal of time staring at screens. You probably know someone who is constantly texting or instant messaging. Perhaps you have a friend who plays computer games for hours on end. Why do people get so attached to their devices? Is it possible to become addicted to these activities?

According to psychiatrist Edward Hallowell, the brains of heavy users of digital devices crave newness, and every text or email message results in a release of the neurotransmitter dopamine that feeds the craving [**150**]. That's why we find it difficult to break away from these activities [**151**].

Another reason people can find it hard to leave their devices is because businesses are trying to keep them attached. The term **attention economy** refers to the idea that the attention of a consumer has economic value. Businesses vie for the attention of consumers through Web sites, social media, and other channels. They use technology to deliver personalized content designed to keep consumers engaged.

3.11.1 Is Internet Addiction Real?

Our electronic devices are like addictive drugs in the sense that when we use them, they provide our brains with immediate positive feedback [**152**]. Psychiatrist Jerald Block maintains that Internet addiction is a common disorder with at least three variants: gaming, "sexual preoccupations," and messaging [**153**]. According to Block, all of these variants share the following characteristics: engaging in excessively long sessions online; becoming angry, tense, or depressed when forced to be away from a device; feeling a need to enhance online experiences by obtaining better equipment or spending more time online; and suffering negative social consequences.

Citing insufficient research data, the American Psychiatric Association did not include Internet addiction in its most recent *Diagnostic and Statistical Manual of Mental Disorders* [**154**]. On the other hand, Internet addiction has been recognized and taken seriously in both South Korea and China since 2007.

The average South Korean high-school student spends 23 hours per week gaming [**155**]. After 10 cardiopulmonary-related deaths in Internet cafeś (Figure 3.2), South Korea began training mental health counselors in how to treat Internet addiction [**156, 157**]. In 2011 the South Korean government passed a law prohibiting children under the age of 16 from accessing online games between midnight and 6 a.m. [**158**].

Figure 3.2

Many South Koreans play online games in centers called PC bangs. In 2005 a 28-year-old South Korean man died after playing one game practically nonstop for 50 hours.

(Kim-Jae Hwan/AFP/Getty Images)

In 2007 the Chinese government issued a regulation limiting people under 18 to three hours of online game play per day, and in 2021 it put in place even stricter limits. Children and teenagers in China are no longer allowed to play online games on school days, and their weekend and holiday game play is limited to one hour per day [**159**].

Our concern in this section is excessive use of digital devices that causes harm. We will use the term "Internet addiction" to describe this behavior because it is the term most widely used by the press, even as we recognize that experts disagree about whether excessive use is a genuine addiction.

3.11.2 Contributing Factors to Addiction

According to Stanton Peele, social, situational, and individual factors can increase a person's susceptibility to addiction. For example, peer groups play an important role in determining how individuals use alcohol and other drugs. People in stressful situations are more likely to become addicted, as are those who lack social support and intimacy, and those who have limited opportunities for "rewarding, productive activity" [**160**]. Individual factors that make a person more

susceptible to addiction include a tendency to pursue an activity to excess, a lack of achievement, a fear of failure, and feelings of alienation.

Kimberly Young's studies led her to "believe that behaviors related to the Internet have the same ability to provide emotional relief, mental escape, and ways to avoid problems as do alcohol, drugs, food, or gambling" [**161**]. She noted that those who are addicted to the Internet are typically addicted to a single application.

3.11.3 Ethical Evaluation of Internet Addiction

People who use digital devices excessively can harm themselves and others for whom they are responsible. For this reason, excessive use of digital devices is a moral issue.

Kantianism, utilitarianism, and social contract theory all share the Enlightenment view that individuals, as rational beings, have the capacity and the obligation to use their critical judgment to govern their lives [**162**]. Kant held that addiction is a vice, because it's wrong to allow your bodily desires to dominate your mind [**163**]. Mill maintained that some pleasures are more valuable than others and that people

have the obligation to help each other distinguish better pleasures from worse ones [**96**]. Ultimately, people are responsible for the choices they make. Even if an addict is "hooked," the addict is responsible for choosing to engage in the activity the first time.

The Enlightenment view assumes that people are capable of controlling their compulsions. According to Jeffrey Reiman, vices are "dispositions that undermine the sovereignty of practical reason. Dispositions, like habits, are hard but not impossible to overcome, and undermining something weakens it without necessarily destroying it entirely" [**162**, p. 89].

Reiman's view is supported by Peele, who believes addicts can choose to recover from their addictions. "People recover to the extent that they (1) believe an addiction is hurting them and wish to overcome it, (2) feel enough efficacy to manage their withdrawal and life without the addiction, and (3) find sufficient alternative rewards to make life without the addiction worthwhile" [**160**, p. 156].

While our analysis to this point has concluded that individual addicts are morally responsible for their addictions, it's also possible for a society to bear some collective moral responsibility for the addictions of some of its members. We

have already discussed how social conditions can increase a person's susceptibility to addiction, and Peele states an addict will not recover unless life without the addiction has sufficient rewards. Some people use digital devices as a way to escape into their own world, because in the "real world" they suffer from social isolation [**164**]. Perhaps we should reflect on whether any of our actions or inactions make certain members of our community feel excluded.

Summary

The Internet and cellular networks are powerful and flexible technologies that have revolutionized communication by making it possible for billions of people to communicate with each other. Never before have so many people around the globe been able to interact: sharing information, engaging in commercial transactions, organizing political movements, competing in online games, helping those in need, and much more. At the same time, those who seek to exploit others have found new ways to do so using these same technologies.

The Web provides a remarkably simple way for people to post and access information, and it now contains several billion indexed pages. The Web has replaced printed encyclopedias and is giving books, journals, and newspapers a run for their money. It contains images of sublime beauty and shocking cruelty, uplifting poetry and expletive-ridden hate speech, well-organized encyclopedias and figments of paranoid imaginations, useful software and hidden computer viruses. In short, it is a reflection of the best and the worst of humanity.

Texting has supported myriad activities, from the social to the deadly serious. It allows friends and family members to check in on each other and set up social encounters, it is an important way for people to make international money transfers without banks, and it has also been used to organize mass protests and overthrow governments.

As social media have become more popular, they have become an increasingly important way for people to get the news. In fact, two-thirds of Americans now read news stories on social media sites, principally Facebook. Facebook's algorithms help ensure people will see news stories that reinforce their views rather than challenge them. For this reason, some commentators fear that Facebook may be harming democracy by increasing political polarization.

Governments have responded to the latent power of these new technologies in a variety of ways. The most repressive governments have made the Internet inaccessible to the masses. Other governments have instituted controls that prevent certain sites from being accessed. To promote social and political stability, the Chinese government prohibits access to certain Internet sites and sometimes restricts cell phone service. On one occasion it shut down the Internet in an entire region for months. In an effort to ensure children

are not exposed to online pornography, the United States government requires libraries to install antipornography filters. Given the focus in the United States on preventing children from being exposed to pornography, it is ironic that many minors have voluntarily created and transmitted explicit images of themselves.

Those who wish to exploit other people have found ways to use these new communication technologies to achieve their ends. Spammers are sending out hundreds of billions of spam emails every day. Others make a living selling stolen credit card information. Millions of people every year are the targets of identity theft.

The challenge for each of us is to reflect on our own actions and ponder whether there are times we may have stepped over the line and put ourselves first, privileging our own needs and desires over those of other people. Cyberbullying and posting revenge porn are the result of decisions made by individuals.

Finally, these new communication technologies have provided new opportunities for people to harm themselves. A good example is the phenomenon commonly referred to as Internet addiction. Some people become so engaged with their digital devices that they spend too much time with their

eyes glued to their screens and too little time taking care of their responsibilities to themselves and to others.

What is the proper governmental response to the Internet addiction crisis? The governments of South Korea and China have put limits on the number of hours per day that children can play online games, and an educational campaign in South Korean schools informs children of the dangers of Internet addiction and encourages healthy alternative activities, such as listening to music.

Further Reading, Listening, and Viewing

Stefana Broadbent. "How the Internet Enables Intimacy." *TEDGlobal 2009*, July 2009. 9:48. www.ted.com/talks/stefana_broadbent_how_the_internet_enab

Malcolm Gladwell. "Small Change: Why the Revolution Will Not Be Tweeted." *New Yorker*, October 4, 2010.

Ted Greenwald. "Under the Influence: How Facebook and Twitter and Candy Crush Get Us Addicted to Swiping and Clicking and Posting." *Wired*, January 2015, pp. 76–77.

David Grossman. "The Rise of 'Fake News,' Manipulation and 'Alternative Facts.'" *BBC Newsnight*, February 6, 2017. 4:27. www.youtube.com/watch?v=1aTApGWVGoI.

Tristan Harris, Ramsay Brown, Larry Rosen, Nancy Cheever, and Gabe Zickermann. "Brain Hacking." Interview by Anderson Cooper. *60 Minutes*, CBS. April 9, 2017. 13:47. www.youtube.com/watch?v=awAMTQZmvPE.

Kashmir Hill. “A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.” *New York Times*, August 21, 2022. https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html.

Mike Rugnetta. “Are Virtual Video Game Economies Becoming Real?” *Idea Channel*, September 19, 2012. 5:26. video.pbs.org.

William Siu. “I Make Video Games. I Won’t Let My Daughters Play Them.” *New York Times*, October 2, 2022. https://www.nytimes.com/2022/10/02/opinion/video-game-addiction.html.

Derek Thompson. “Be Your Selves.” *1843*, April/May 2017. www.1843magazine.com/technology/be-your-selves.

Ali Velshi. “How Fake News Grows in a Post-Fact World.” *TEDxQueensU*, March 9, 2017. 18:23. www.youtube.com/watch?v=nkAUqQZCyrM.

Bill Wasik. “Welcome to the Programmable World.” *Wired*, June 2013.

Judy Woodruff. “Google’s Schmidt and Cohen Discuss the Digital Future.” *PBS NewsHour*, May 2, 2013. 9:38. video.pbs.org.

Judy Woodruff. “Spotting the Fakes Among the Five-Star Reviews.” *PBS NewsHour*, January 19, 2015. 9:30. video.pbs.org.

“High Speed Internet Is Connecting Palau Women to New Opportunities.” *Asian Development Bank*, March 20, 2018. www.adb.org/news/videos/high-speed-internet-connecting-palau-women-new-opportunities.

“Mobile Money: Kenyans Talk About How M-PESA Has Changed Their Lives.” WorldRemit, March 29, 2017. 2:43. www.youtube.com/watch?v=QKjofAUhSso.

Review Questions

1. Nearly all spam is blocked by spam filters. Why does sending spam continue to be so popular?
2. Why has spam's share of email traffic been in decline since 2009?
3. Many commercial enterprises support both Web sites and mobile apps. Why?
4. What are the similarities and the differences between texting and instant messaging?
5. How have social media affected the news people are exposed to?
6. How has the Internet undermined traditional print newspapers?
7. Define censorship in your own words.
8. What characteristics of the Internet make the censorship of Internet content difficult?
9. Why do broadcasters in the United States have more limited First-Amendment rights than book publishers?

10. How has sexting by teens created new legal challenges?
11. What is the leading form of identity theft?
12. Why are college students particularly vulnerable to identity theft?
13. Give two examples of high-tech methods of identity theft and two examples of low-tech methods of identity theft.
14. Define cyberbullying in your own words.
15. What physiological reason has been given for the difficulty some people experience detaching themselves from their digital devices?
16. What is the Enlightenment view regarding responsibility for addiction?

Discussion Questions

17. Facebook's username policy requires each Facebook user to use "the name they go by in everyday life" [**165**]. The policy forbids the use of professional or religious titles, phrases instead of names, and offensive words. Many Indigenous people have had their accounts deactivated for supposedly using a fake name, including Dana Lone Hill, Shane Creepingbear, and Lance Brown Eyes [**166**]. Meanwhile, people who set up accounts with phony but plausible usernames have not had their usernames challenged. Should Facebook require every user to use their real name? If so, what would be a fair way to enforce this requirement?

18. Why is instant messaging or texting more popular among young adults than making phone calls?

19. Why is "cold calling" considered to be an acceptable sales practice, but spamming isn't?

20. Internet service providers monitor their chat rooms and expel users who violate their codes of conduct. For example, users can be kicked off for insulting a person or a group of people based on their race, religion, or sexual orientation. Is it wrong for an ISP to expel someone for hate speech?

21. Stockbrokers are now required to save all their instant messaging communications. Is having a record of everything you type good or bad? Do you think this requirement will change the behavior of brokers?

22. There is a thriving "real-world" market for gold, artifacts, and avatars from virtual worlds such as World of Warcraft. In effect, rich Westerners are offshoring game playing to China. Do you find this image disturbing?

23. What are the benefits and harms of Internet censorship?

24. Do you ever read a newspaper? If so, how often? If not, how do you get your news? How do you know that the news you consume is accurate?

25. Should the tax dollars of citizens of democratic nations be used to help people in authoritarian nations get

around the Web censorship of their repressive governments?

26. Should people publishing accusations against others on their blogs or Facebook pages be held responsible if they disseminate false information?

27. Should a college or university have the right to suspend students who brag about breaking its rules on their Facebook pages?

28. In September 2012, Joseph Aziz, a graduate student at Montclair State University in New Jersey, posted a YouTube video in which he said that a fellow student's legs look like "a pair of bleached hams." The university disciplined Aziz for violating the university's code of conduct, ordered him to avoid all contact with the other student, and forbade him from posting anything else about the other student on social media. After being disciplined, Aziz complained about the gag order in a private group on Facebook and made a joke about escaping the other student's "tyrannical ham lock." A member of the Facebook group copied Aziz's comments to university administrators, who then gave Aziz a one-semester suspension that appears on his

official college transcript [**167**]. Was the response of Montclair State University appropriate?

29. Discuss similarities and differences between the Web and each of these other ways that we communicate: the telephone system, physical mail, bookstores, movie theaters, newspapers, broadcast and cable TV. Should governments ignore the Web, or should they regulate it somehow? If governments should regulate the Web, should the regulations be similar to the regulations for one of the aforementioned communication systems, or should they be unique in significant ways?

30. The convenience of *Wikipedia* makes it a popular reference for students. After several instances in which students cited incorrect information, however, the history department at Middlebury College prohibited references to *Wikipedia* articles in papers or exams. Did the Middlebury history department go too far? What is the proper role, if any, for *Wikipedia* in academic research?

31. Should bloggers be given the same rights as newspaper, magazine, or television journalists?

32. Should children be prevented from accessing some Web sites? Who should be responsible for the actions of

children surfing the Web?

33. Are there any circumstances under which sexting is morally acceptable?

34. What is the age at which a parent or guardian should provide a child with a cell phone? Should younger children be provided with cell phones having fewer features?

35. Review the exchange in Section 3.10.7 between Hunter Moore, creator of a Web site featuring revenge porn, and one of the women whose image had appeared on the site without her permission. Who has the more compelling argument? Why? If you could ask Hunter Moore a follow-up question, what would it be? If you could ask the woman a follow-up question, what would it be?

36. Discuss the morality of Google's page-ranking algorithm. Does it systematically exclude Web pages containing opinions held only by a small segment of the population? Should every opinion on the Web be given equal consideration?

37. What is the longest amount of time you have ever spent in a single game session on a smartphone, tablet, or computer? Have you ever been so engrossed in a game

that you ignored bodily needs, such as eating or going to the bathroom?

38. Should Grand Theft Auto or Call of Duty be pulled off store shelves and not marketed to children?

39. In the United States television commercials for cigarettes are banned. Should there be a ban on commercials for violent video games?

40. The income of companies providing persistent online games depends on the number of subscribers they attract. Since consumers have a choice of many products, each company is motivated to create the best possible experience for its customers. Role-playing adventures have no set length. When playing one of these games, it's easy to spend more time on the computer than originally planned. Some subscribers cause harm to themselves and others by spending too much time playing these games. Should the designers of persistent online games bear some moral responsibility for this problem?

41. The governments of South Korea and China have taken action to restrict the number of hours per day children can access online games. Should our government take similar action?

42. A school district forbids students from using their cell phones on school buses, but many students ignore this rule. A frustrated bus driver installs a cell phone jammer on his bus. When the jammer is turned on, cell phones within 40 feet stop working. (The use of jammers is against the law.) The bus driver says, "The kids think they are sneaky by hiding low in their seats and using their phones. Now the kids can't figure out why their phones don't work, but can't ask because they will get in trouble! It's fun to watch them try to get a signal" [**168**].

    Discuss the morality of the bus driver's use of the jammer.

43. According to some commentators, Facebook and Twitter played a vital role in the Arab Spring uprising because they made it possible for activists to organize large protests in a short amount of time. Others argue that Facebook and Twitter were simply tools used by activists and that genuine social grievances led to the revolutions in Tunisia and Egypt. What is your view?

44. After popular uprisings in Tunisia and Egypt in 2011, the US government said it would spend $30 million to fund the development of new services and technologies

designed to allow activists in other countries to get around Internet restrictions imposed by their governments.

Announcing this initiative, Secretary of State Hillary Clinton said, "We are convinced that an open Internet fosters long-term peace, progress and prosperity. The reverse is also true. An Internet that is closed and fractured, where different governments can block activity or change the rules on a whim—where speech is censored or punished, and privacy does not exist—that is an Internet that can cut off opportunities for peace and progress and discourage innovation and entrepreneurship" [**169**].

Should the US government provide activists in other countries the tools to get around Internet restrictions imposed by authoritarian governments?

45. In July 2011, activists shut down a San Francisco subway station as a way of protesting the death of a drunk man shot by a Bay Area Rapid Transit (BART) police officer [**170**]. A month later, the subway system blocked cell-phone service at several stations in an effort to prevent another protest. BART officials said protesters were planning to use their mobile devices to coordinate their activities and keep track of police

movements. The agency pointed out that civil disturbances at crowded subway stations during rush hour could create unsafe conditions for commuters, BART employees, and the protesters themselves [**171**].

Was BART justified in blocking cell-phone service?

46. What role do online reviews play in your life as a consumer? Do you find online reviews to be more reliable or less reliable than reviews from friends and family members?

In-Class Exercises

47. Divide the class into groups. Each group should come up with a variant of the case study "Anh the Acme Accountant," in which both a Kantian evaluation and an act-utilitarian evaluation would conclude Anh did something wrong.

48. Divide the class into groups. Each group should come up with a variant of the case study "Kate's Blog," in which the analysis from the perspective of social contract theory would conclude Kate did nothing wrong, but an act-utilitarian evaluation would conclude Kate did something wrong.

49. Divide the class into teams representing each of the following groups:

    - Small, struggling business
    - Large, established corporation
    - Internet service provider
    - Consumer

Discuss the value of direct email versus other forms of advertising, such as direct mail, television advertising, radio advertising, the Yellow Pages, and setting up a Web site.

50. A company uses pop-up advertising to market its software product, which blocks popups from appearing when someone is surfing the Web. Debate the morality of the company's marketing strategy.

51. Ad-blocking software attachments to Web browsers enable a Web surfer to visit Web sites without having to view the pop-up advertisements associated with these Web pages. Debate this proposition: "People who use ad-blocking software are violating an implicit 'social contract' with companies that use advertising revenues as a means of providing free access to Web pages."

52. In 2000 the Estonian parliament passed a law declaring Internet access to be a fundamental human right of its citizens. Divide the class into two groups (pro and con) to debate the following proposition: Internet access should be a fundamental human right, along with such other fundamental human rights as the right to life and the right to free speech.

53. How do you determine the credibility of information you get from the Web? How would you rank the reliability of information provided by each of the following sources of Web pages? Does the type of information you're seeking affect your ranking?
    - Establishment newspaper
    - Counterculture newspaper
    - Television network
    - Corporation
    - Nonprofit organization
    - Individual
54. Martin Dula has suggested that parents should not provide their children with phones capable of taking photos and videos because these phones tempt children to participate in sexting [**93**].

Divide the class into groups of four or five students. Each group should discuss the proposition: Parents and legal guardians should not allow their children under the age of 16 to own cell phones capable of taking, transmitting, or receiving photographs or videos. After

a reasonable amount of time, teams should take turns sharing their conclusions with the rest of the class.

References

[1] Jill Cowan, Shawn Hubler, and Ivan Penn. "California Leaders Credit Cellphone Alert for Sudden Conservation." *New York Times*, September 7, 2022. https://www.nytimes.com/2022/09/07/us/california-power-grid-cellphone-alert.html.

[2] Tavneet Suri and William Jack. "The Long-run Poverty and Gender Impacts of Mobile Money." *Science*, 354(6317): 1288–1292, December 9, 2016.

[3] "#StatusOfMind: Social Media and Young People's Mental Health and Wellbeing." Royal Society for Public Health, London, 2017. www.rsph.org.uk/uploads/assets/uploaded/62be270a-a55f-4719- ad668c2ec7a74c2a.pdf.

[4] Craig Silverman and Lawrence Alexander. "How Teens in the Balkans Are Duping Trump Supporters with Fake News." *BuzzFeed*, November 3, 2016. www.buzzfeed.com.

[5] Ivan Simic. "Top 10 Highest-Viewed Esports Events of 2022." *Esports Insider*, December 26, 2022.

esportsinsider.com/2022/12/highest-viewed-esports-events-2022.

[6] "Email Statistics Report: 2020-2024 --- Executive Summary." *Radicati Group*, February 2020. www.radicati.com.

[7] Brad Templeton. "Origin of the Term 'Spam' to Mean Net Abuse." Templetons.com, July 8, 2005. www.templetons.com/brad/spamterm.html.

[8] Peter H. Lewis. "An Ad (Gasp!) in Cyberspace." *New York Times*, April 19, 1994.

[9] Joanne Pimonova. "Email Spam Trends at a Glance: 2001–2012." *EmailTray*, June 5, 2012. www.email.tray.com.

[10] Darya Gudkova and Maria Namestnikova. "Spam Evolution 2011." *Kaspersky Security Bulletin*, March 1, 2012. securelist.com.

[11] Justin M. Rao and David H. Reiley. "The Economics of Spam." *Journal of Economic Perspectives*, 26(3): 87–110, Summer 2012.

[12] Henry Dalziel. "Costs of Nefarious Services from the Underground Cybercriminal World." November 15, 2012. www.concise-courses.com.

[13] Saul Hansell. “Internet Is Losing Ground in Battle Against Spam.” *New York Times*, April 22, 2003.

[14] Joe Stewart. “Top Spam Botnets Exposed.” Dell SecureWorks, April 8, 2008. www.secureworks.com/research/threats/topbotnets.

[15] Elena Bondarenko, Darya Gudkova, and Maria Namestnikova. “Spam Evolution 2010.” *Kaspersky Security Bulletin*, February 17, 2011. securelist.com.

[16] Tatyana Kulikova, Roman Dedenok, Olga Svistunova, Andrey Kovtun, and Irina Shimko. “Spam and Phishing in 2022.” Securelist (Web site), February 16, 2023. securelist.com.

[17] Brian Whitworth and Elizabeth Whitworth. “Spam and the Social-Technical Gap.” *Computer*, 37(10): 38–45, October 2004.

[18] Tim Berners-Lee. *Weaving the Web*. HarperCollins Publishers, New York, NY, 1999.

[19] Gianni Catlfamo. “The Death of the Browser.” *KetchumBlog*, February 19, 2011. blog.ketchum.com.

[20] “Quarterly Retail E-Commerce Sales.” *United States Census* Bureau, May 18, 2023. www.census.gov.

[21] Craig Newmark. Craigslist (Web site). Accessed March 17, 2018. www.craigslist.org/about/craig_newmark.

[22] S. Dixon. “Most Popular Social Networks Worldwide as of January 2023, Ranked by Number of Monthly Active Users.” Statista (Web site), February 14, 2023. www.statista.com.

[23] Nicola Clark. “Selecting a Seatmate to Make Skies Friendlier.” *New York Times*, February 24, 2012.

[24] Daniel H. Pink. “The Book Stops Here.” *Wired*, page 125, March 2005.

[25] Paul Festa. “Dialing for Bloggers.” *New York Times*, February 25, 2003.

[26] Clive Thompson. “Spooked: Using Darknets to Foil the NSA.” *Wired*, November 2013.

[27] “Get the Best Route, Every Day, with Real-Time Help from Other Drivers.” Waze, Inc., June 17, 2013. www.waze.com.

[28] Kickstarter (Web site). Accessed July 5, 2023. www.kickstarter.com.

[29] Jimmy Yap. “Power Up!” *Internet Magazine*, February 2003.

[30] David Barboza. “Ogre to Slay? Outsource It to China.” *New York Times*, December 9, 2005.

[31] Carlos Hernández. “The Gold Game: Farming Virtual Money to Fight a Real-Life Crisis.” *Caracas Chronicles*, September 21, 2017. www.caracaschronicles.com.

[32] “Experience Smart Home Awesomation.” *Revolv*, June 14, 2013. revolv.com.

[33] “Returns Filed, Taxes Collected & Refunds Issued.” Internal Revenue Service (Web site), April 14, 2023. www.irs.gov.

[34] “Global Online Gambling Market Report 2023: Increasing Availability of High-Speed Internet Drives Growth - ResearchAndMarkets.com.” *Business Wire*, April 19, 2023. www.businesswire.com.

[35] Kiva (Web site). Accessed March 20, 2018. www.kiva.org.

[36] “Cryptocurrencies: What Are They?” Charles Schwab (Web site), June 13, 2022. https://www.schwab.com/learn/story/cryptocurrencies-what-are-they.

[37] Andy Greenberg. “Crypto Currency.” *Forbes*, April 20, 2011.

[38] Katharina Buchholz. “These Are the Countries Where Cryptocurrency Use Is Most Common.” World Economic Form (Web site), February 18, 2021. https://www.weforum.org/agenda/2021/02/how-common-is-cryptocurrency/.

[39] Markus Jakobsson and Ari Juels. “Proofs of Work and Bread Pudding Protocols (Extended Abstract).” In B. Preneel, editor. *Secure Information Networks: IFIP—The International Federal for Information Processing*, vol. 23. Springer, Boster, MA. https://doi.org/10.1007/978-0-387-35568-9_18.

[40] Jake Frankenfield. “Bitcoin Mining.” Investopedia (Web site), April 26, 2023. https://www.investopedia.com/terms/b/bitcoin-mining.asp.

[41] “Bitcoin Energy Consumption Index.” Digiconimist (Web site). Accessed July 24, 2023. https://digiconomist.net/bitcoin-energy-consumption.

[42] Ouyang Shijia. “China to Tighten Virtual Currency Mining Regulation.” *China Daily*, November 16, 2021. http://www.chinadaily.com.cn/a/202111/16/WS6193513ba310

[43] E. Napoletano. “Proof of Stake Explained.” *Forbes Advisor*, February 16, 2023. https://www.forbes.com/advisor/investing/cryptocurrency/proo of-stake/.

[44] “What Is Proof of Stake?” McKinsey & Company, January 3, 2023. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is- proof-of-stake.

[45] “Ethereum Energy Consumption Index.” Digiconimist (Web site), Accessed July 24, 2023. https://digiconomist.net/ethereum-energy-consumption.

[46] “Processing 24,000 Visa Transactions per Second: How It’s Done.” Unibul’s Money Blog (Web site), Accessed July 24, 2023. https://blog.unibulmerchantservices.com/processing-24000-visa- transactions-per-second-how-its-done/.

[47] Ethan Wolff-Mann. “‘Only Good for Drug Dealers’: More Nobel Prize Winners Snub Bitcoin.” Yahoo!Finance, April 27, 2018. https://finance.yahoo.com/news/good-drug-dealers-nobel-prize-winners- snub-bitcoin-184903784.html.

[48] Emma Newbery. “5 Cryptocurrencies That Have Failed —and Why.” *The Ascent*, August 13, 2021.

https://www.fool.com/the-ascent/cryptocurrency/articles/5-cryptocurrencies-that-have-failed-and-why/.

[49] Kalley Huang. “Why Did FTX Collapse? Here’s What to Know.” *New York Times*, November 18, 2022. https://www.nytimes.com/2022/11/10/technology/ftx-binance-crypto-explained.html.

[50] “51% Attacks.” Digital Currency Initiative, Massachusetts Institute of Technology, Accessed July 24, 2023. https://dci.mit.edu/51-attacks.

[51] Bloomberg. “China Says All Cryptocurrency Transactions Are Illegal.” *TIME*, September 24, 2021. https://time.com/6101328/china-outlaw-cryptocurrency/.

[52] Tolu Oguniesi and Stephanie Busari. “Seven Ways Mobile Phones Have Changed Lives in Africa.” *CNN*, September 12, 2012. www.cnn.com.

[53] S. Dixon. “Twitter - Statistics & Facts.” Statistica (Web site), March 21, 2023. www.statistica.com.

[54] Chris Chase. “Germany’s World Cup Rout of Brazil Was the Most Tweeted Event in History.” *USA Today*, July 9, 2014. ftw.usatoday.com.

[55] Claire Cain Miller. “Mom-and-Pop Operators Turn to Social Media.” *New York Times*, July 23, 2009.

[56] Clay Shirky. “The Political Power of Social Media.” *Foreign Affairs*, January/February 2011.

[57] Philip N. Howard. “The Arab Spring’s Cascading Effects.” *Pacific Standard*, February 23, 2011. www.psmag.com.

[58] “Region in Turmoil.” Al Jazeera. Accessed August 8, 2011. blogs.aljazeera.net/twitter-dashboard.

[59] William Saletan. “Springtime for Twitter.” *Slate*, July 18, 2011. www.slate.com.

[60] Malcolm Gladwell. “Small Change: Why the Revolution Will Not Be Tweeted.” *New Yorker*, October 4, 2011.

[61] Penagiotis Takis Metaxas and Eni Mustafaraj. “From Obscurity to Prominence in Minutes: Political Speech and Real-Time Search.” In *Web Science Conference 2010*. Raleigh, NC, April 26–27, 2010.

[62] “How George Floyd Died, and What Happened Next.” *New York Times*, July 29, 2022. https://www.nytimes.com/article/george-floyd.html.

[63] Rachel Treisman. “Darnella Frazier, Teen Who Filed Floyd’s Murder, Praised for Making Verdict Possible.” *National Public Radio*, April 21, 2021. https://www.npr.org/sections/trial-over-killing-of-george- floyd/2021/04/21/989480867/darnella-frazier-teen-who-filmed-floyds- murder-praised-for-making-verdict-possib.

[64] Larry Buchanan, Quoctrung Bui, and Jugal K. Patel. “Black Lives Matter May Be the Largest Movement in U.S. History.” *New York Times*, July 3, 2020. https://www.nytimes.com/interactive/2020/07/03/us/george-floyd-protests-crowd-size.html.

[65] Alana Wise, Camila Domonoske, and Rachel Treisman. “Where It Stands: Election Hinges on Key States, Final Results May Take a While.” *NPR*, November 3, 2020. Updated November 4, 2020. https://www.npr.org/2020/11/03/931042936/biden-secures-early-electoral- vote-lead-but-swing-state-crown-jewels-still-in-pl.

[66] Dan Barry and Sheera Frenkel. “‘Be There. Will Be Wild!’: Trump All but Circled the Date.” *New York Times*, January 6, 2021.

https://www.nytimes.com/2021/01/06/us/politics/capitol-mob-trump-supporters.html.

[67] Jane Lytvynenko and Molly Hensley-Clancy. "The Rioters Who Took Over the Capitol Have Been Planning Online in the Open for Weeks." *BuzzFeed.News*, January 6, 2021. https://www.buzzfeednews.com/article/janelytvynenko/trump-rioters-planned-online.

[68] Maggie Haberman. "Trump Told Crowd 'You Will Never Take Back Our Country with Weakness.'" *New York Times*, January 6, 2021. Updated January 15, 2021. https://www.nytimes.com/2021/01/06/us/politics/trump-speech-capitol.html.

[69] Ryan Lucas. "Where the Jan. 6 Insurrection Investigation Stands, One Year Later." *NPR*, January 6, 2022. https://www.npr.org/2022/01/06/1070736018/jan-6-anniversary-investigation-cases-defendants-justice.

[70] Michael Kunzelman. "Capitol Rioters' Social Media Posts Influencing Sentencing." *AP News*, December 11, 2021. https://apnews.com/article/media-prisons-social-

media-capitol-siege- sentencing-0a60a821ce19635b70681faf86e6526e.

[71] Mathew Ingram. “How Google and Facebook Have Taken Over the Digital Ad Industry.” *Fortune*, January 3, 2017. fortune.com.

[72] Daisuke Wakabayashi and Mike Isaac. “In Race Against Fake News, Google and Facebook Stroll to the Starting Line.” *New York Times*, January 25, 2017.

[73] United States of America v. Internet Research Agency et al. United States District Court for the District of Columbia. Criminal No. 18 U.S.C. SS 2, 371, 1349, 1028A. February 16, 2018.

[74] Case Newton. “Russia’s Election Posts Reached 126 Million People, Facebook Will Tell Congress.” *The Verge*, October 30, 2017.

[75] Richard Gunther, Eric C. Nisbet, and Paul Beck. “Trump May Owe His 2016 Victory to ‘Fake News,’ New Study Suggests.” *The Conversation*, February 15, 2018. theconversation.com.

[76] Hunt Alcott and Matthew Gentzkow. “Social Media and Fake News in the 2016 Election.” *Journal of*

Economic Perspectives, 31(2): 211–236, Spring 2017. web.stanford.edu/~gentzkow/research/fakenews.pdf.

[77] Anamitra Deb, Stacy Donohue, and Tom Glaisyer. "Is Social Media a Threat to Democracy?" The Omidyar Group, October 1, 2017.

[78] Elisa Shearer and Jeffrey Gottfried. "News Use Across Social Media Platforms 2017." Pew Research Center, September 7, 2017. www.journalism.org.

[79] Cass Sunstein. *Republic.com*. Princeton University Press, Princeton, NJ, 2001.

[80] Dan Kennedy. "Print Is Dying, Digital Is No Savior: The Long, Ugly Decline of the Newspaper Business Continues Apace." *WGBH News*. January 26, 2016. news.wgbh.org.

[81] Pew Research Center. "State of the News Media 2015." April 2015. www.pewresearch.org.

[82] Christine Haughney. "New York Times Company Sells Boston Globe." *New York Times*, August 3, 2013.

[83] Robert G. Kaiser. "The Bad News About the News." *The Brookings Essay*, October 16, 2014. csweb.brookings.edu.

[84] Thomas Jefferson. Letter to Edward Carrington, January 16, 1787.

[85] Elaine C. Kamarck and Ashley Gabriele. “The News Today: 7 Trends in Old and New Media.” Center for Effective Public Management, Brookings, November 2015. www.brookings.edu.

[86] Eason Jordan. “News We Kept to Ourselves.” *New York Times*, April 11, 2003.

[87] “About Filtering.” OpenNet Initiative, August 1, 2007. opennet.net/about-filtering.

[88] “North Korea: Internet Usage, Broadband and Telecommunications Reports.” *Internet World Stats*, January 15, 2023. www.internetworldstats.com.

[89] “Freedom on the Net 2017: Saudi Arabia.” Freedom House. Accessed May 7, 2018. freedomhouse.org/report/freedom-net/2017/saudi-arabia.

[90] Rebekah Heacock. “China Shuts Down Internet in Xinjiang Region after Riots.” OpenNet Initiative, July 6, 2009. opennet.org.

[91] Asher Moses. “Censoring Mobiles and the Net: How the West Is Clamping Down.” *Sydney Morning Herald*, August 15, 2011. www.smh.com.au.

[92] “Internet Filtering in China.” OpenNet Initiative, June 15, 2009. opennet.net.

[93] “Freedom on the Net 2017: China.” *Freedom House*. Accessed May 7, 2018. freedomhouse.org/report/freedom-net/2017/china.

[94] “IOC Agrees to Internet Blocking at the Games.” *New York Times*, July 30, 2008.

[95] Immanuel Kant. “What Is Enlightenment?” In *Foundations of the Metaphysics of Morals*. Library of Liberal Arts, Upper Saddle River, NJ, 1997.

[96] John Stuart Mill. “On Liberty.” In *On Liberty and Utilitarianism*. Bantam Books, New York, NY, 1993.

[97] Edward G. Hudon. *Freedom of Speech and Press in America*. Public Affairs Press, Washington, DC, 1963.

[98] Francis Canavan. *Freedom of Expression: Purpose as Limit*. Carolina Academic Press, Durham, NC, 1984.

[99] Cass R. Sunstein. *Democracy and the Problem of Free Speech*. Free Press, New York, NY, 1993.

[100] George Carlin. “Filthy Words.” On *Occupation: Foole*, Atlantic Records, 1973.

[101] Supreme Court of the United States. Federal Communications Commission v. Pacifica Foundation et al., 438 US 726 (1978).

[102] “Parent- Controlled Filtering Software.” Irvine Unified School District, Orange County, California. Accessed October 5, 2013. www.iusd.org.

[103] Associated Press. “Justices Uphold Use of Internet Filters in Public Libraries.” *NYTimes.com*, June 23, 2003.

[104] Jeffrey Kosseff. “Libraries Should Bar Web Porn, Court Rules.” *Oregonian* (Portland, OR), June 24, 2003.

[105] James Rachels. *The Elements of Moral Philosophy*. 4th ed. McGraw-Hill, Boston, MA, 2003.

[106] John Rawls. *A Theory of Justice*. Revised Edition, p. 187. Belknap Press of Harvard University Press, Cambridge, MA, 1999.

[107] Lorenne Clark. “Sexual Equality and the Problem of an Adequate Moral Theory: The Poverty of Liberalism.” In *Contemporary Moral Issues*. McGraw-Hill Ryerson, Toronto, ON, 1997.

[108] Langdon Winner. "Electronically Implanted 'Values.'" *Technology Review*, 100(2), February/March 1997.

[109] Doug Johnson. "Internet Filters: Censorship by Any Other Name?" *Emergency Librarian*, 25(5), May/June 1998.

[110] "Teen Online & Wireless Safety Survey: Cyberbullying, Sexting, and Parental Controls." *Cox Communications*, May 2009.

[111] Michele Ybarra. "How Many Teens Are Actually Sexting? Why Teen Sexting Rates Are Overreported in the Media." *Psychology Today*, January 19, 2015. www.psychologytoday.com.

[112] Mike Celizic. "Her Teen Committed Suicide over 'Sexting.'" *TodayShow.com*, March 6, 2009. www.msnbc.msn.com.

[113] Kim Zetter. "'Sexting' Hysteria Falsely Brands Educator as Child Pornographer." *Wired*, April 3, 2009. www.wired.com.

[114] Martin Dula. "Sexting: The Convergence of Two Revolutions." *Pop Culture History* (blog), June 25, 2009. www.greathistory.com.

[**115**] Justin W. Patchin. "The Status of Sexting Laws Across the United States." Cyberbullying Research Center (Web site). https://cyberbullying.org/the-status-of-sexting-laws-across-the-united- states.

[**116**] Dorothy E. Denning. *Information Warfare and Security*, p. 241. Addison-Wesley, Boston, MA, 1999.

[**117**] Javelin. "Identity Fraud Hits All Time High with 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study." February 6, 2018. www.javelinstrategy.com/press-release/identity-fraud-hits-all-time- high-167-million-us-victims-2017-according-new-javelin.

[**118**] Javelin Strategy & Research. "2009 Identity Fraud Survey Report: Consumer Version." February 2009. www.javelinstrategy.com.

[**119**] Steve Weisman. "Why College Students Are at High Risk of Identity Theft." *FTPress*, October 3, 2013. www.ftpress.com.

[**120**] David McGuire. "Bush Signs Identity Theft Bill." *WashingtonPost.com*, July 15, 2004.

[**121**] Myles Anderson. "Local Consumer Review Survey 2014." July 1, 2014. www.brightlocal.com.

[122] Logan Kugler. “Keeping Online Reviews Honest.” *Communications of the ACM*, Vol 57(11): 20–23, November 2014.

[123] Judy Woodruff. “Spotting the Fakes Among the Five-Star Reviews.” *PBS NewsHour*, January 19, 2015. 9:30. video.pbs.org.

[124] Craig Smith. “26 Important Kik Messenger Statistics and Facts (January 2018).” DMR, March 31, 2018. expandedramblings.com.

[125] Steve Jefferson and Emma Koch. “Police Issue Warning About Child Predators Using Kik App.” *NBC33 News*, August 22, 2013. www.21alive.com.

[126] Dave Spencer. “Police: Kik App Used by Sexual Predator to Lure West Michigan Teen to Home.” *Fox17 News*, January 14, 2014. fox17online.com.

[127] Howard Koplowitz. “Whisper App Rape: Ronald Peterson III Arrested for Allegedly Raping 12-Year-Old Washington Girl He Met through Secrets App.” *International Business Times*, October 22, 2013. www.ibtimes.com.

[128] Colleen Curry. “Underage Sex Sting Nabs 40 Would-Be Pedophiles.” *20/20*, January 18, 2012.

abcnews.go.com.

[129] Phil Perry. “Lincolnton PD Nabs 17 in Child Predator Sting Operation.” *Lincoln Times-News*, May 22, 2015. www.lincolntimesnews.com.

[130] Mark Boyle. “Galveston Task Force Agents Arrest Child Sexual Predators in Sting Operation.” Click2Houston (Web site). Accessed June 22, 2015. www.click2houston.com.

[131] Noah Pransky. “Officers Accused of Bending Rules on Sex Sting Arrests.” *USA Today*, August 8, 2014. www.usatoday.com.

[132] Tiffany Hsu and Sapna Maheshwari. “The Titanic Truthers of TikTok.” *New York Times*., June 16, 2023. https://www.nytimes.com/2023/06/16/business/titanic-tiktok-misinformation.html.

[133] Andy Baio. “Finding the Star Wars Kid.” *Waxy.org* (blog), May 13, 2003. waxy.org.

[134] Tu Thanh Ha. “Parents File Lawsuit over Star Wars Video.” *Globe and Mail*, Toronto, Ontario, Canada, July 23, 2003.

[135] “Star Wars Kid Is Top Viral Video.” *BBC News*, November 27, 2006. www.bbc.co.uk.

[136] Steve Pokin. "'MySpace' Hoax Ends with Suicide of Dardenne Prairie Teen." *Suburban Journals*, November 11, 2007. suburbanjournals.stltoday.com.

[137] "Parents Want Jail Time for MySpace Hoax Mom." *ABC News*, November 29, 2007. abcnews.go.com.

[138] Kim Zetter. "Government's Star Witness Stumbles: MySpace Hoax Was Her Idea, Not Drew's." *Wired*, November 20, 2008. www.wired.com.

[139] "Missouri Begins Prosecuting Under Cyberbullying Law." *Fox News*, December 20, 2008. www.foxnews.com.

[140] Kim Zetter. "Lori Drew Not Guilty of Felonies in Landmark Cyberbullying Trial." *Wired*, November 26, 2008. www.wired.com.

[141] Kim Zetter. "Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury." *Wired*, July 2, 2009. www.wired.com.

[142] Congressional Research Service. "H. R. 1966: Megan Meier Cyberbullying Prevention Act (Summary)." April 2, 2009. www.govtrack.us.

[143] "revenge porn" (entry). *Collins English Dictionary*. www.collinsdictionary.com.

[144] "Exposed Women Confront Website Owner: 'What Is Your Motive?'" *Anderson*, November 21, 2011. 1:28. www.youtube.com/watch?v=GAcXjjD3nYg.

[145] Debbie L. Sklar. "It's 2.5 Years in Fed Prison for 'Revenge Porn' Website King." *My News LA*, December 2, 2015. mynewsla.com.

[146] "'Revenge Porn' Conviction Is a First Under California Law." *LA Times*, December 4, 2014. www.latimes.com.

[147] Abby Ohlheiser. "Reddit's New Privacy Policy Bans Sharing Nude Images Without Consent." *Washington Post*, February 24, 2015. www.washingtonpost.com.

[148] "The Twitter Rules." Twitter (Web site). Accessed July 12, 2015. support.twitter.com/entries/18311.

[149] Amit Singhal. "'Revenge Porn' and Search." June 19, 2015. googlepublicpolicy.blogspot.com.

[150] Jacky Lynne A. Oiga. "Is Technology Driving You Crazy?" *Mania Bulletin*, August 20, 2013. www.mb.com.ph.

[151] Susan Weinschenk. "100 Things You Should Know About People: #8—Dopamine Makes You Addicted to

Seeking Information." *What Makes Them Click: Applying Psychology to Understand How People Think, Work, and Relate* (blog), November 7, 2009. www.whatmakesthemclick.net.

[152] Carolyn Gregoire. "Our Digital Device Addiction Is Causing 'A National Attention Deficit.'" *Huffington Post*, October 7, 2014. www.huffingtonpost.com.

[153] Jerald J. Block. "Issues for DSM-V: Internet Addiction." *American Journal of Psychiatry*, March 2008. psychiatryonline.org.

[154] American Psychiatric Association. "DSM-5 Proposed Revisions Include New Category of Addiction and Related Disorders; New Category of Behavioral Addictions Also Proposed" (press release). February 10, 2010.

[155] B. N. Kim. "From Internet to 'Family-Net': Internet Addict vs. Digital Leader." 2007 International Symposium on the Counseling and Treatment of Youth Internet Addiction, Seoul, Korea, 2007.

[156] Y. H. Choi. "Advancement of IT and Seriousness of Youth Internet Addiction." 2007 International

Symposium on the Counseling and Treatment of Youth Internet Addiction, Seoul, Korea, 2007.

[157] D. H. Ahn. “Korean Policy on Treatment and Rehabilitation for Adolescents’ Internet Addiction.” 2007 International Symposium on the Counseling and Treatment of Youth Internet Addiction, Seoul, Korea, 2007.

[158] Melia Robinson. “Korea’s Internet Addiction Crisis Is Getting Worse, as Teens Spend Up to 88 Hours a Week Gaming.” *Business Insider*, March 25, 2015. www.businessinsider.com.

[159] Chris Buckley. “China Tightens Limits for Young Online Gamers and Bans School Night Play.” *New York Times*, August 30, 2021. https://www.nytimes.com/2021/08/30/business/media/china-online-games.html.

[160] Stanton Peele. *The Meaning of Addiction: An Unconventional View*. Jossey-Bass, San Francisco, CA, 1998.

[161] Kimberly S. Young. “Internet Addiction: Symptoms, Evaluation, and Treatment.” In L. VandeCreek and T.

L. Jackson editors. *Innovations in Clinical Practice*, vol. 17. Professional Resource Press, Sarasota, FL, 1999.

[162] Jeffrey Reiman. *Critical Moral Liberalism: Theory and Practice*. Rowman & Littlefield Publishers, Lanham, MD, 1997.

[163] Immanuel Kant. *Lectures on Ethics*. Cambridge University Press, Cambridge, England, 2001.

[164] Mark Griffiths. "Does Internet and Computer 'Addiction' Exist? Some Case Study Evidence." *CyberPsychology and Behavior*, 3(2), 2000.

[165] "What Names Are Allowed on Facebook?" Facebook (Web site). Accessed May 26, 2018. www.facebook.com/help/112146705538576.

[166] ICT Staff. "Facebook Name Police: Native American Names Aren't 'Authentic' Enough." *Indian Country Today*, February 13, 2015. indiancountrymedianetwork.com.

[167] John Del Signore. "NJ Student Suspended for 'Trolling' on YouTube, Facebook." *Gothamist* (blog), January 16, 2013. gothamist.com.

[168] Matt Richtel. “Devices Enforce Silence of Cellphones, Illegally.” *New York Times*, November 4, 2007. www.nytimes.com.

[169] US Department of State. “Internet Freedom.” *Fact sheet*, February 15, 2011. www.state.gov.

[170] “Protesters Angry About Police Shooting Shut Down S.F. Subway Stop.” *CNN*, July 12, 2011. www.cnn.com.

[171] “S.F. Subway System Admits Cutting Cellphone Service to Stop Planned Protest.” *CNN*, August 13, 2011. news.blocks.cnn.com.

Chapter 4

Intellectual Property

4.1 Introduction

AFTER JIMMY FALLON INVITED ALLISON RAE ONTO *THE TONIGHT show* to demonstrate eight popular TikTok dances, social media erupted with protests. Why? Because the show did not recognize or provide any compensation to the choreographers of the dances, most of whom were Black people. Fallon responded to the criticism by inviting the creators of the dances onto *The Tonight Show* the following week to talk with him and perform their dances [**1, 2**].

At a Bowling for Soup concert, the band made up a song onstage. According to singer Jaret Reddick, “That thing was on YouTube before I even got back home from the show” [**3**]. Do entertainers have the right to control who sees and hears a performance of their music?

DALL- E 2 is an AI system that generates realistic images based on user prompts. The system gained its abilities by being trained on 650 million images [**4**]. Should artists and photographers receive some compensation for creating the images used to train DALL-E 2?

Over 100 million Netflix subscribers worldwide were sharing their passwords with people outside their households. In 2022 Netflix began cracking down on password sharing in Argentina, the Dominican Republic, El Salvador, Guatemala, and Honduras, making out-of-household users get their own accounts. In 2023 Netflix extended its effort to Canada, New Zealand, Portugal, Spain, and the United States. Netflix subscribers had the option of adding an extra member outside their household—for an additional monthly charge, of course [5].

As a society, we benefit from access to high-quality television shows, music, movies, computer programs, and other products of the human intellect. These products are efficiently distributed using the modern information technology infrastructure. However, the same infrastructure also makes it easier for people to gain access to these products without paying for them. When this happens, producers of intellectual property do not receive all the payments the law says they are entitled to. The legal system has responded by giving more rights to the creators of intellectual property. Are these changes in the best interests of our society, or are politicians catering to special interest groups?

In this chapter we discuss how information technology is affecting our notions of intellectual property. We consider what makes intellectual property different from tangible property and how governments have created a variety of mechanisms to guarantee intellectual property rights. We examine what has been considered "fair use" of intellectual property created by others, and how new copy protection technologies are eroding the notions of fair use. Meanwhile, peer-to-peer networks are making it easier than ever for consumers to get access to music and movies without purchasing them, putting pressure on companies selling these products to make obtaining a legal copy at least as easy as obtaining an illegal copy. We also explore the evolution of intellectual property protection for computer software and the rise of the open-source movement, which advocates the distribution of source code to programs. Finally, we take a look at one organization's efforts to make it easier for artists, musicians, and writers to use the Internet as a vehicle for stimulating creativity and enhancing collaboration.

4.2 Intellectual Property Rights

According to the World Intellectual Property Organization, **intellectual property** "refers to creations of the mind: inventions; literary and artistic works; and symbols, names and images used in commerce" [6]. Examples of intellectual property include essays, poems, novels, plays, movies, songs, drawings, paintings, photographs, architectural designs, industrial designs, inventions, chemical formulas, and computer programs.

It is important to distinguish between intellectual property and its physical manifestation in some medium. If a poet composes a new poem, for example, the poem itself is the intellectual property, not the piece of paper on which the poem is printed.

In most of the world there is a widely accepted notion that people have the right to own property. Does this right extend to intellectual property as well? To answer this question, we need to examine the philosophical justification for a natural right to property.

4.2.1 Property Rights

The English philosopher John Locke (1632–1704) developed an influential theory of property rights. In *The Second Treatise of Government*, Locke makes the following case for a natural right to property. First, people have a right to property in their own person. Nobody has a right to the person of anybody else. Second, people have a right to their own labor. The work that people perform should be to their own benefit. Third, people have a right to those things that they have removed from Nature through their own labor [7].

For example, suppose you are living in a village, in the middle of woods that are held in common. One day you walk into the woods, chop down a tree, saw it into logs, and split the logs into firewood (Figure 4.1). Before you cut down the tree, everyone had a common right to it. By the time you have finished splitting the logs, you have mixed your labor with the wood, and at that point it has become your property. Whether you burn the wood in your stove, sell it to someone else, pile it up for the winter, or give it away, the choice of what to do with the wood is yours.

Figure 4.1

According to John Locke, people have a natural right to the things they

Locke uses the same reasoning to explain how a person can gain the right to a piece of land. Taking a parcel out of the state of Nature by clearing the trees, tilling the soil, and planting and harvesting crops gives people who performed these labors the right to call the land their property.

To Locke, this definition of property makes sense as long as two conditions hold. First, no person claims more property than they can use. In the case of harvesting a natural resource, it is wrong for someone to take so much that some of it is wasted. For example, people should not appropriate more land than they can tend. Second, when people remove something from the common state in order to make it their own property, there is still plenty left over for others to claim through their labor. If the woods are full of trees, I can chop a tree into firewood without denying you or anyone else the opportunity to do the same thing.

Locke's description of a natural right to property is most useful at explaining how virtually unlimited resources are initially appropriated. It is not as useful in situations where there are limited resources left for appropriation.

4.2.2 Extending the Argument to Intellectual Property

Is there a natural right to intellectual property?

We can try to demonstrate that such a right exists by extending Locke's theory of property rights to intellectual property. However, since Locke was talking about the ownership of physical objects and we are talking about the ownership of creative expressions, we must resort to an analogy. We'll compare writing a play to making a belt buckle [8]. In order to make a belt buckle, a person must mine ore, smelt it down, and cast it. To write a play, a playwright "mines" words from the English language, "smelts" them into stirring prose, and "casts" them into a finished play.

Attempting to treat intellectual property the same as ordinary property leads to certain paradoxes, as Michael Scanlan has observed [8]. We consider two of Scanlan's scenarios illustrating problems that arise when we extend Locke's natural-rights argument to intellectual property.

Scenario A, Act 1

After a day of rehearsals at the Globe Theatre, William Shakespeare decides to have supper at a pub across the street. The pub is full of gossip about royal intrigue in Denmark. After his second pint of beer, Shakespeare is visited by the muse, and in an astonishing burst of energy, he writes *Hamlet* in one fell swoop.

If we apply Locke's theory of property to this situation, clearly Shakespeare has the right to own *Hamlet*. He mixed his labor with the raw resources of the English language and produced a play. Remember, we're not talking about the

piece of paper upon which the words of the play are written. We're talking about the sequence of words comprising the play. The paper is simply a way of conveying them.

What should Shakespeare get from his ownership of *Hamlet*? Here are two ideas (you can probably think of more): He should have the right to decide who will perform the play. He should have the right to require others who are performing the play to pay him a fee.

So far, so good. But let's hear the end of the story.

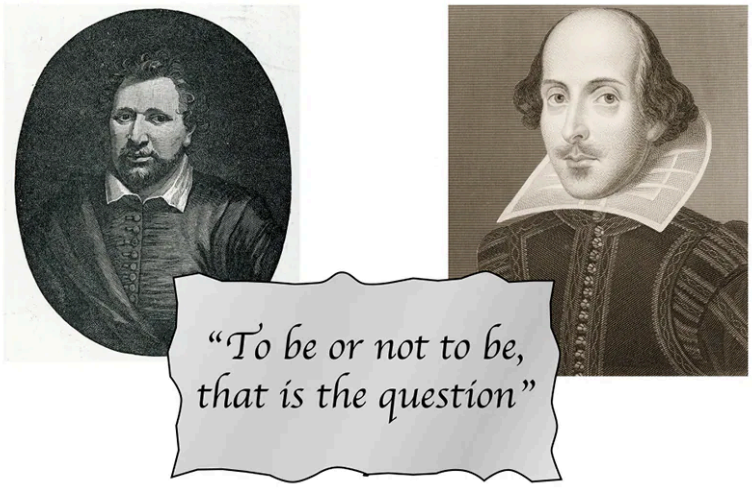
Scenario A, Act 2

On the very same night, Ben Jonson, at a pub on the opposite side of London, hears the same gossip, is struck by the same muse, and writes *Hamlet*—exactly the same play!

Ben Jonson has mixed his intellectual labor with the English language to produce a play. According to Locke's theory of

natural rights to property, he ought to own it. Is it possible for both Ben Jonson and William Shakespeare to own the same play (Figure 4.2)? No, not as we have defined ownership rights. It is impossible for both of them to have the exclusive right to decide who will perform the play. Both of them cannot have an exclusive claim to royalties collected when *Hamlet* is performed. We've uncovered a paradox: two people labored independently and produced only a single artifact.

Figure 4.2



Suppose both Ben Jonson and William Shakespeare simultaneously write down *Hamlet*. Who owns it?

(Ben Jonson, Walker Art Library/Alamy Stock Photo; Shakespeare, Classic Image/Alamy Stock Photo)

We ended up with this paradox because our analogy is imperfect. If two people go to the same iron mine, dig ore, smelt it, and cast it into belt buckles, there are two belt buckles, one for each person. Even if the belt buckles look identical, they are distinct, and we can give each person ownership of one of them. This is not the case with *Hamlet*. Even though Jonson and Shakespeare worked independently, there is only one *Hamlet*: the sequence of words that constitute the play. Whether we give one person complete ownership or divide the ownership among the two men, both cannot get full ownership of the play, which is what they ought to have if the analogy were perfect. Therefore, the uniqueness of intellectual properties is the first way in which they differ from physical objects.

A second paradox has to do with the copying of intellectual property. Consider a slightly different version of our story.

Scenario B

One evening William Shakespeare stays up all night in a pub writing *Hamlet* while Ben Jonson goes to a

party. The next morning Shakespeare returns to the Globe Theatre, but he carelessly leaves a copy of *Hamlet* in the pub. Jonson stops by for breakfast, sees the manuscript, transcribes it, and walks out the door with a copy of the play in his possession, leaving the original copy where it was.

Did Jonson steal *Hamlet*? Shakespeare still has his physical copy of the play, but he has lost exclusive control over who will read, perform, or hear the play. If you want to call this stealing, then stealing intellectual property is quite different from stealing a physical object. When you steal someone's car, they can't drive it anymore. When you steal someone's joke, both of you can tell it.

Certainly, any creator of a piece of intellectual property has the right to keep his ideas a secret. After Shakespeare wrote *Hamlet*, he could have locked it in a trunk to prevent others from seeing it. Ben Jonson would not have had the right to break into Shakespeare's trunk to get access to the play. Hence we can argue that there is a natural right to keep an idea confidential. Unfortunately, this is a weak right because Shakespeare cannot perform the play while he is keeping it

confidential. He must give up the confidentiality in order to put his creation to good use.

We began this section with the following question: Is there a natural right to intellectual property? We have found no right other than the weak right to keep an idea confidential. In our quest for stronger rights, we have uncovered two important differences between tangible property and intellectual property. First, every intellectual property is one-of-a-kind. Second, copying a piece of intellectual property is different from stealing a physical object.

4.2.3 Benefits of Intellectual Property Protection

New ideas in the form of inventions and artistic works can improve the quality of life for the members of a society. Some people are altruistic and will gladly share their creative energies. For example, Benjamin Franklin (1706–1790) invented many useful items, including an improved wood stove, the lightning rod, the odometer, and bifocals. He did not patent any of them. Franklin said, “As we enjoy great advantages from the invention of others, we should be glad

of an opportunity to serve others by any invention of ours; and this we should do freely and generously" [9, p. 28]. However, most people find the allure of money to be a strong inducement for laboring long hours in the hope of creating something useful. So even if there are no natural rights to intellectual property, a society may choose to grant intellectual property rights to people because of the beneficial consequences.

The authors of the Constitution of the United States recognized the benefits society reaps by encouraging creativity. Article I, Section 8, of the US Constitution gives Congress the power to "promote the Progress of Science and useful Arts by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."

If a person has the right to control the distribution and use of a piece of intellectual property, there are many opportunities for that person to make money. For example, suppose you build a better mousetrap and the government gives you ownership of this design. You may choose to manufacture the mousetrap yourself. Anyone who wants the better mousetrap must buy it from you, because no other mousetrap manufacturer has the right to copy your design. Alternatively,

you may choose to license your design to other manufacturers, who will pay you for the right to build mousetraps according to your design. It is also possible for you to be rewarded for your creativity without the new device ever reaching the public. Suppose you sell an exclusive license for your better mousetrap to the company that dominates the mousetrap market. The company chooses not to manufacture the new mousetrap because—for whatever reason—it can make more money selling the existing technology. In this situation you and the company benefit, but society is deprived access to the new, improved technology.

4.2.4 Limits to Intellectual Property Protection

Society benefits the most when inventions are in the public domain and anyone can take advantage of them. Going back to the mousetrap example, we would like everyone in society who needs a mousetrap to get the best possible trap. If someone invents a superior mousetrap, the maximum benefit would result if all mousetrap manufacturers were able to use the better design. On the other hand, if the inventor of the superior mousetrap did not have any expectation of profiting

from her new design, they might not have bothered to invent it. Hence there is a tension between the need to reward the creators of intellectual property by giving them exclusive rights to their ideas and the need to disseminate these ideas as widely as possible.

The way Congress has traditionally addressed this tension is through a compromise. It has granted authors and inventors exclusive rights to their writings and discoveries but only for a limited period of time. (Note: Rights to a piece of intellectual property produced by an employee in the normal course of their duties belong to the employer.) At the end of that time period, the intellectual property enters the public domain. While creators have control over the distribution of their properties, use of the properties is more expensive, and the creators are rewarded. After properties enter the public domain, using them becomes less expensive, and everyone has the opportunity to produce derivative works from them.

Consider a community orchestra that wishes to perform a piece of classical music. It may purchase a piece of music from the public domain for far less money than it cost simply to rent the same piece of music while it was still protected by copyright (Table 4.1).

Table 4.1

Artist	*Work*	*Previous Rental Fee*	*Year Became Public Domain*	*Purchase Price*
Ravel	Daphnis et Chloe Suite No. 1	$450.00	1987	$155.00
Ravel	Mother Goose Suite	540.00	1988	70.00
Ravel	Daphnis et Chloe Suite No. 2	540.00	1989	265.00
Griffes	The White Peacock	335.00	1993	42.00
Puccini	O Mio Babbino Caro	252.00	1994	26.00
Respighi	Fountains of Rome	441.00	1994	140.00
Ravel	Le Tombeau de Couperin	510.00	1995	86.00
Respighi	Ancient Aires and Dances Suite No. 1	441.00	1996	85.00
Elgar	Cello Concerto	550.00	1997	140.00
Holst	The Planets	815.00	1997	300.00
Ravel	Alborada Del Gracioso	360.00	1999	105.00

Once a piece of classical music enters the public domain, it may be purchased for much less than it cost simply to rent the same piece of music for two performances when it was still under copyright protection. These prices assume the orchestra has an annual budget of $150,000 or less **[10]**.

(Table from "Letter to The Honorable Senator Spencer Abraham," by Randolph P. Luck from Luck's Music Library. Copyright © 1996 by Randolph P. Luck. Reprinted with permission.)

The question is, what is a reasonable length of time to grant authors and inventors exclusive rights to their creative works? Supreme Court justice Stephen Breyer [**11**], Kembrew McLeod [**12**], and Lawrence Lessig [**13**] all cited "Happy Birthday to You" as evidence that copyright protections are excessive. "Happy Birthday to You," based on a tune from 1893, is one of the most popular songs in the world, but for more than 50 years, it was almost never heard on television. That's because more than a century after "Happy Birthday" was first sung, music publisher Warner/Chappell owned the copyright to the song, and television networks had to pay

licensing fees to Warner/Chappell to air it. In the early 21st century, Warner/Chappell was collecting about $2 million in licensing income each year from public performances of "Happy Birthday to You" [**14**].

As it turns out, the focus on "Happy Birthday to You" led to a surprising outcome. In a meticulously researched article, George Washington University law professor Robert Brauneis concluded that the song was "almost certainly no longer under copyright, due to a lack of evidence about who wrote the words; defective copyright notice; and a failure to file a proper renewal application" [**15**]. After the publication of Brauneis's article, the production company of documentary filmmaker Jennifer Nelson filed a class action complaint asking the court to "declare invalid the copyright that defendant Warner/Chappell claims to own to the world's most popular song, *Happy Birthday to You*" [**16**]. In 2016 the US District Court for the Central District of California declared "Happy Birthday to You" to be in the public domain. Warner/Chappell agreed to pay up to $14 million to settle claims of a class who had paid licensing fees as far back as 1949 [**17**].

)

4.3 Protecting Intellectual Property

While the US Constitution gives Congress the right to grant authors and inventors exclusive rights to their creations, it does not elaborate on how these rights will be protected. Today there are four different ways in which individuals and organizations protect their intellectual property: trade secrets, trademarks/service marks, patents, and copyrights.

4.3.1 Trade Secrets

A **trade secret** is a confidential piece of intellectual property that provides a company with a competitive advantage. Examples of trade secrets include formulas, processes, proprietary designs, strategic plans, customer lists, and other collections of information. The right of a company to protect its trade secrets is widely recognized by governments around the world. In order to maintain its rights to a trade secret, a company must take active measures to keep it from being discovered. For example, companies typically require

employees with access to a trade secret to execute a confidentiality agreement.

A famous trade secret is the formula for Coca-Cola syrup. The formula is locked inside a vault at the World of Coca-Cola in Atlanta, Georgia. Only a few people within the company know the entire formula, and they have signed nondisclosure agreements. The task of making the syrup is divided among different groups of employees. Each group makes only one part of the final mixture, so that nobody in these groups learns the complete recipe.

An advantage of trade secrets is that they do not expire. A company never has to disclose a trade secret. Coca-Cola has kept its formula secret for more than 100 years.

The value of trade secrets is in their confidentiality. Hence trade secrets are not an appropriate way to protect many forms of intellectual property. For example, it makes no sense for a company to make a movie a trade secret, because a company can only profit from a movie by allowing it to be viewed, which makes it no longer confidential. On the other hand, it is appropriate for a company to make the *idea* for a movie a trade secret. Art Buchwald pitched Paramount Pictures a story called *King for a Day*, about an African prince who visits the United States. After the studio produced

the movie *Coming to America*, starring Eddie Murphy, Buchwald successfully sued Paramount for breach of contract, because he had made the studio sign a confidentiality agreement before he gave them the plot [18].

While it is illegal to steal a trade secret, there are other ways in which confidentiality may be broken. Reverse engineering is one way in which a competing firm can legally gain access to information contained in a trade secret. If another company can purchase a can of Coca-Cola and figure out the formula, it is free to manufacture a soft drink that looks and tastes just like Coke. However, it wouldn't be able to sell its soft drink as Coca-Cola or Coke, because those names are trademarked, as explained in the next section.

Another way in which a competing firm can gain access to information contained in another company's trade secret is by hiring its employees. While a firm can require its employees to sign confidentiality agreements, it cannot erase the memories of an employee who starts working for a competing firm. Hence some "leakage" of confidential information may be inevitable when employees move from one company to another.

4.3.2 Trademarks and Service Marks

A **trademark** is a word, symbol, picture, sound, or color used by a business to identify goods. A **service mark** is a mark identifying a service. Hereafter, we will use the word "trademark" to mean either a trademark or a service mark. By granting a trademark, a government gives a company the right to use it and the right to prevent other companies from using it. Through the use of a trademark, a company can establish a "brand name." Society benefits from branding because branding allows consumers to have more confidence in the quality of the products and services they purchase [**19**].

In the United States, trademarks are registered through the US Patent and Trademark Office. Trademarks must be chosen carefully, because not every mark can be registered, and even marks that are registered may be impossible to protect. The US Patent and Trademark Office simply registers trademarks; defending them is up to the trademark's owner. Obtaining a trademark requires choosing the mark, identifying the goods and/or services that will be identified by the mark, searching the US Patent and Trademark Office database to determine if a similar mark has already been

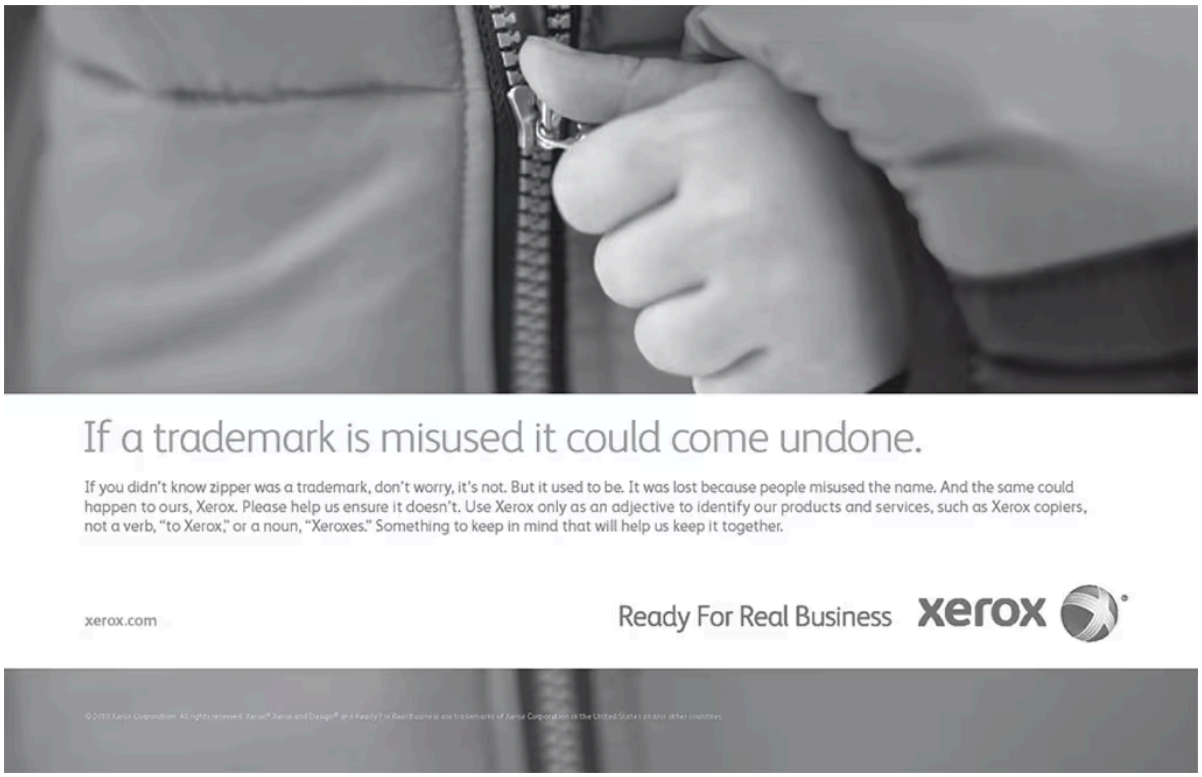
registered for comparable goods and/or services, and demonstrating that the mark is being used or about to be used in commerce. Firms often retain trademark attorneys to help them navigate these steps [20].

When a company is the first to market a distinctive product, it runs the risk that its brand name will become a common noun used to describe any similar product. When this happens, the company may lose its right to exclusive use of the brand name. Some trademarks that have become common nouns are yo-yo, aspirin, escalator, thermos, and brassiere.

In order to protect their trademarks, companies strive to ensure their marks are used as adjectives rather than nouns or verbs. One way they do this is through advertising (Figure 4.3). Kimberly-Clark's advertisements refer to "Kleenex *brand* facial tissue." Remember Johnson & Johnson's jingle, "I am stuck on Band-Aid *brand* 'cause Band-Aid's stuck on me"? Another way companies protect their trademarks is by contacting those who are misusing them. For example, Adobe has responded to Web posts about "photoshopping images" by posting this follow-up message: "The Photoshop trademark must never be used as a common verb or as a noun. The Photoshop trademark should always be capitalized

and should never be used in possessive form, or as a slang term" [21].

Figure 4.3


If a trademark is misused it could come undone.
If you didn't know zipper was a trademark, don't worry, it's not. But it used to be. It was lost because people misused the name. And the same could happen to ours, Xerox. Please help us ensure it doesn't. Use Xerox only as an adjective to identify our products and services, such as Xerox copiers, not a verb, "to Xerox," or a noun, "Xeroxes." Something to keep in mind that will help us keep it together.
xerox.com
Ready For Real Business
xerox

Xerox Corporation ran this advertisement as part of its campaign to protect its trademark.

(Courtesy of Xerox Corporation.)

4.3.3 Patents

A **patent** is how the US government provides intellectual property protection for a limited period of time to creators of machines, systems, and other inventions. A patent is quite different from a trade secret because a patent is a public document that provides a detailed description of the invention. The owner of the patent can prevent others from

making, using, or selling the invention for the lifetime of the patent, which is currently 20 years. After the patent expires, anyone has the right to make use of its ideas.

Obtaining a patent is a lengthy, complicated, and expensive process. In the United States, the inventor must go through several steps before filing an application with the US Patent and Trademark Office. The first step is to determine if the invention is patentable. You cannot file a patent application for an invention that is already being used or that has already been described in a publication or another patent application. Even if the invention is different from an invention that has already been described, patented, or used, the patent application may still be refused if the differences are deemed to be obvious to a person familiar with the technical area of the invention. Finally, the invention must serve a useful purpose and be designed so that it can accomplish that purpose. Because the patent application process requires specialized knowledge, the US Patent and Trademark Office recommends that those seeking patents get expert help from a registered patent attorney or patent agent [22].

Bell Telephone Company

Alexander Graham Bell's patent on the telephone enabled the Bell Telephone Company to create a monopoly on telephone

services in the United States. A key to the early success of the company was its decision to lease, rather than sell, telephones to customers. When Bell's original patents on the telephone expired in 1894, other companies were free to make telephones, and about 6,000 phone companies sprang up across the United States [**23**].

The Bell Telephone Company evolved into the American Telephone and Telegraph Company (AT&T), which became one of the world's largest corporations. In 1974 the US Department of Justice sued AT&T for antitrust violations. The case was settled in 1982, and in 1984 seven regional telephone companies, nicknamed "the Baby Bells," took over AT&T's local phone services. AT&T continued to manufacture equipment and offer long-distance telephone service [**23**].

Polaroid v. Kodak

Dr. Edwin Land invented "instant" photography. The company he founded, Polaroid Corporation, had many patents protecting the invention of film that developed in 60 seconds. Polaroid did not license these patents to other firms, and for many years it was the only company to sell cameras and film allowing photographs to be developed in a minute.

When Kodak introduced its first instant camera in 1976, Polaroid sued Kodak for infringement of 10 of its patents. In 1985 a federal district court ruled that Kodak had infringed on seven of Polaroid's patents, and a federal appeals court upheld the ruling in 1986 [**24**]. Kodak paid Polaroid a $925 million settlement and got out of the instant photography business [**25**].

Cleartype

Sometimes companies see an advantage in licensing their inventions. For example, Microsoft invented a software technology called ClearType that improves the clarity of text displayed on liquid crystal displays (LCDs), screens often used in smartphones, tablets, laptops, and computer monitors. The ClearType technology is protected by 10 US patents. In 2003 Microsoft announced it would begin licensing more of its inventions to other companies, and Agfa Monotype Corp. in Belgium became the first company to license ClearType [**26, 27**]. The royalty rate was $1 per unit for personal digital assistants, $2 per unit for personal computers, and $3 per unit for tablets. The total amount of revenue Microsoft expected to make from the technology was not enough to have a significant impact on the company's balance sheet, leading some observers to conclude Microsoft

was opening up its patent portfolio to other companies to reduce pressure from antitrust regulators in the United States and the European Union [26].

4.3.4 Copyrights

A **copyright** is how the US government provides authors with certain rights to original works that they have written. The owner of a copyright has five principal rights:

1. The right to reproduce the copyrighted work
2. The right to distribute copies of the work to the public
3. The right to display copies of the work in public
4. The right to perform the work in public
5. The right to produce new works derived from the copyrighted work

Copyright owners have the right to authorize others to exercise these five rights with respect to their works. Here are two examples. The owner of a copyright to a play may sell a license to a high-school drama club that wishes to perform it. After a radio station broadcasts a song, it must pay the songwriter(s) and the composer(s) through a performance rights organization such as ASCAP, BMI, or SESAC.

Copyright owners also have the right to prevent others from infringing on their rights to control the reproduction, distribution, display, performance, and production of works derived from their copyrighted work.

Several important industries in the United States, including the motion picture, music, software, and book publishing industries, rely on copyright law for protection. "Copyright industries" account for nearly 8 percent of the US gross domestic product, with over $1.8 trillion in sales. Nearly 10 million US citizens work in these industries, which are growing at a much faster rate than the rest of the US economy. With foreign sales and exports of $230 billion, copyright industries were the leading export sector in the United States in 2022 [**28**].

In this section we examine court cases and legislation that have helped define the limits of copyright in the United States.

Gershwin Publishing v. Columbia Artists

Columbia Artists Management, Inc. (CAMI) managed concert artists, and it sponsored hundreds of local, nonprofit community concert associations that arranged concert series featuring CAMI artists. CAMI helped the associations

prepare budgets, select artists, and sell tickets. CAMI printed the programs and sold them to the community concert associations. In addition, all musicians performing at these concerts paid CAMI a portion of their fees.

On January 9, 1965, the CAMI-sponsored Port Washington (NY) Community Concert Association put on a concert that included Gershwin's "Bess, You Is My Woman Now" without obtaining copyright clearance from Gershwin Publishing Corporation. The American Society of Composers, Authors, and Publishers (ASCAP) sued CAMI for infringement of copyright.

CAMI argued that it was not responsible for the copyright infringement, since the concert was put on by the Port Washington Community Concert Association. However, the US District Court for the Southern District of New York ruled that CAMI could be held liable because it was aware that the community concert associations it supported were not obtaining proper copyright clearances. In 1971 the US Court of Appeals for the Second Circuit upheld the ruling of the district court [**29**].

Davey Jones Locker

Richard Kenadek ran a computer bulletin board system (BBS) called Davey Jones Locker. Subscribers paid $99 a year for access to the BBS, which contained copies of more than 200 commercial programs. In 1994 Kenadek was indicted for infringing on the copyrights of the owners of the software. He pleaded guilty and was sentenced to six months' home confinement and two years' probation [30].

No Electronic Theft Act

Another incident in 1994 led to further legislation protecting copyrights. David LaMacchia, an MIT student, posted copyrighted software on a public bulletin board he created on a university computer. According to prosecutors, bulletin-board users downloaded more than a million dollars' worth of software in less than two months. However, the prosecutors were forced to drop charges against LaMacchia because he had made the programs available for free. Since he had not profited from his actions, he had not violated copyright law. To close this legal loophole, Congress passed the No Electronic Theft Act of 1997, which made it a criminal offense simply to reproduce or distribute more than a thousand dollars' worth of copyrighted material in a six-month period.

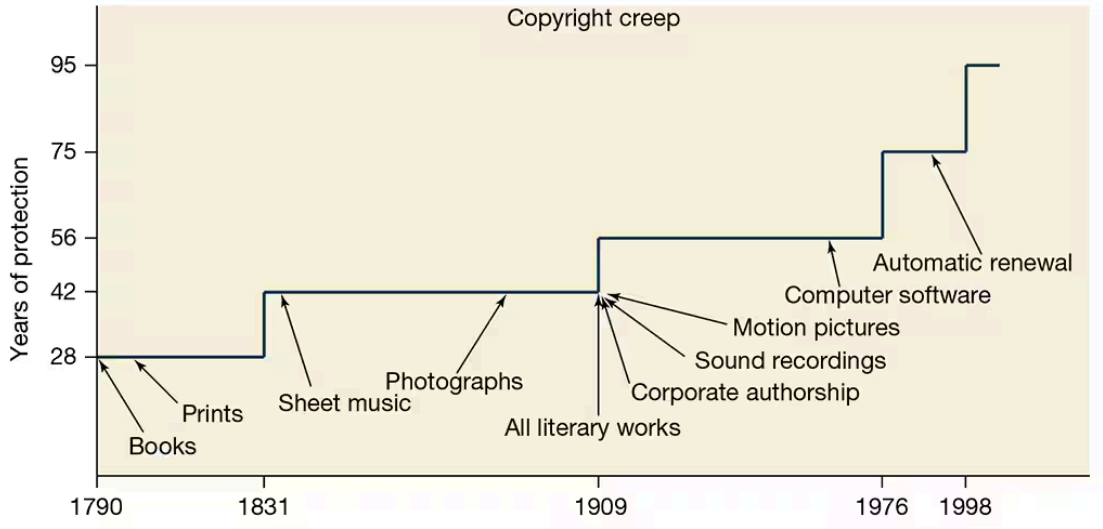
Copyright Creep

As a result of the Sonny Bono Copyright Term Extension Act of 1998, works created and published before January 1, 1978, are protected for 95 years. Works created on or after January 1, 1978, are protected for the author's lifetime plus 70 years after the author's death. If the work is a work made for hire, the length of protection is 95 years from the date of publication or 120 years from the date of creation, whichever is less.

According to Siva Vaidhyanathan, "in the early republic and the first century of American legal history, copyright was a Madisonian compromise, a necessary evil, a limited, artificial monopoly, not to be granted or expanded lightly" [**31**, p. 24]. Over time, however, Congress has gradually increased both the term of copyright protection and the kind of intellectual properties that are protected by copyright (Figure 4.4). One reason has been the desire to have international copyright agreements. In order to complete these agreements, Congress has had to reconcile American copyright law with European law, which in general has had much stronger protections for the producers of intellectual property [**31**]. Another reason for "copyright creep" has been the

introduction of new technologies, such as photography, audio recording, and video recording.

Figure 4.4



Since the first Copyright Act was passed in 1790, both the length of copyright protection and the kinds of intellectual property that can be copyrighted have grown dramatically.

For example, since 1831 music publishers have been able to copyright sheet music and collect royalties from musicians performing this music in public. In 1899 Melville Clark introduced the Apollo player piano, which played songs recorded on rolls of heavy paper. Apollo manufactured and sold piano rolls of copyrighted songs. White-Smith Music Company sued Apollo for infringing on its copyrights. In 1908 the Supreme Court ruled that Apollo had not infringed on White-Smith Music's copyrights. The court suggested that Congress ought to change copyright law if it wanted owners of copyrights to have control over recordings such as piano

rolls and phonograph records. Congress responded by revising the Copyright Act in 1909. The new copyright law recognized that player piano rolls and phonograph records could be copyrighted.

Some people believe the expansion of the scope of copyright protection has tilted the balance of private versus public rights too far toward the copyright holders. They say it is no coincidence that copyright terms were extended just before Mickey Mouse was to enter the public domain. The Walt Disney Corporation lobbied Congress to pass the Sonny Bono Copyright Term Extension Act (CTEA) of 1998, protecting its profits derived from Mickey Mouse, Donald Duck, and its other famous characters [**32**]. Some critics suggest that since Walt Disney made a great deal of money on *Snow White and the Seven Dwarfs, Cinderella, Pinocchio, The Hunchback of Notre Dame, Alice in Wonderland*, and *The Jungle Book*, all based on stories taken from the public domain, it's only fair that at some point Walt Disney characters become part of the public domain, available for others to use in new creative works [**33**].

Eric Eldred, who digitizes old books and makes them freely available over the Web, led a group of petitioners who challenged the CTEA. They argued that the US Constitution

gives Congress the power to grant exclusive rights to authors for "limited times," and that the writers of the Constitution expected copyright durations to be short. By extending the terms of existing copyrights 11 times in 40 years, they said, Congress had exceeded its constitutional power [**34**].

The government and groups representing the entertainment industry, including the Walt Disney Co., the Motion Picture Association of America, and the Recording Industry Association of America, argued that Congress does have the constitutional authority to extend the terms of existing copyrights [**35**].

In a 7–2 decision, the US Supreme Court ruled in favor of the government and the entertainment industry, stating that the petitioners did not demonstrate how the CTEA had crossed "a constitutionally significant threshold." In the opinion of the Court, "Those earlier Acts did not create perpetual copyrights, and neither does the CTEA" [**36**].

Sure enough, the US Congress did not extend the length of copyrights further, and in 2024 Disney's *Steamboat Willie* entered the public domain, along with the original, rat-like Mickey Mouse character appearing in that short film.

Disney continued to hold a trademark on the more modern version of Mickey Mouse as a brand identifier.

4.3.5 Non-fungible Tokens

A **non-fungible token** (NFT) is a digital asset stored on a blockchain and connected with a unique digital asset, such as art, music, or virtual real estate. By contrast, Bitcoins and other cryptocurrencies are fungible or interchangeable with each other.

NFTs can be sold and traded. Typically, the owner of an NFT is licensed to use the asset but does not own the copyright to the asset. For example, in 2021 Christie's auction house sold for $69 million an NFT representing a collage of 5,000 images from the digital artist Beeple [37]. Meanwhile, any Internet user could view the images in the collage for free.

Some have likened owning an NFT to owning an autographed print. Others referred to the NFT phenomenon as a speculative bubble [38]. Prices of NFTs soared between 2019 and 2021, then crashed by the summer of 2022.

4.3.6 Case Study: The Database Guru

Rajiv worked for five years as a software engineer at Felicity Software, a company that sells database systems to consumers and small businesses. During his time at Felicity, Rajiv implemented some clever software optimizations that significantly improved the performance of the database systems sold by Felicity. The company treated the optimizations as trade secrets. It labeled the software as confidential information and took measures to restrict access to the source code to Rajiv and a few other software engineers who helped Rajiv implement and test the system.

On his first day with Felicity, Rajiv had signed an employee confidentiality and proprietary rights agreement. Signing this agreement was a condition of his employment. In this agreement Rajiv had indicated that he understood and acknowledged the following:

1. He would have access to confidential, secret, and proprietary information related to Felicity's business.
2. Felicity placed "great competitive importance and commercial value" on its ability to reserve confidential

information for its exclusive use.

3. Confidential information he developed would be covered by this agreement.

4. He would not "directly or indirectly disclose, publish, communicate or make available" confidential information to anyone outside of the company.

5. His obligations under the agreement would "continue during and after his employment" by Felicity [39].

After completing the database project at Felicity, Rajiv began looking for the opportunity to join a software start-up. With a good reputation in the tight-knit local tech community and strong references from coworkers and managers who praised his talent, work ethic, honesty, and teamwork skills, Rajiv quickly found employment at Unrelated.com, a start-up company in a nearby office park.

Unrelated.com plans to support people doing genealogical research. It is developing a proprietary database system that will be used to store genealogical information. Unrelated.com has no plans to sell the database software. Instead, its income will be derived from the monthly fee users pay in order to access the company's database through the Web or a mobile app. The sales and marketing team estimates that within

three years Unrelated.com could reach a steady state of 50,000 subscribers paying $10 a month, as long as the system performs well. Up to 20 percent of the customers may be using the system during peak periods, which means in order to reach a steady state of 50,000 customers, the database system must be capable of quickly responding to queries from 10,000 users accessing the system simultaneously. If the performance of the system falls short of this goal, fewer people will subscribe to the service. For example, a system that can provide good service to only 5,000 concurrent users will support only 25,000 subscriptions.

Rajiv's title at Unrelated.com is vice president of software, and he earns a salary of $150,000 supervising several teams of software developers. One of these teams is responsible for implementing the genealogical database system and optimizing its performance. As the project progresses, Rajiv realizes that some of the technical solutions proposed by the members of his team are not as good as the solutions he developed for Felicity's database product. The team's preliminary software implementation is unlikely to result in a database system with satisfactory performance when it is being accessed by more than about 5,000 users. In Rajiv's judgment, significant optimizations are needed before the

system is ready to deploy if Unrelated.com is to reach its goal of 50,000 monthly subscribers.

Rajiv believes he has two viable alternatives. The first option is to follow a "clean-room" strategy. He would isolate himself from the team's work product, but he would provide the team with publicly available information on database optimization strategies—in other words, the books, journal articles, and conference papers he benefited from when he implemented the database system optimizations at Felicity. Based on his expertise, Rajiv would also provide the team with realistic performance targets that the various components of the database system should be able to meet.

The second option is to become personally involved in making the necessary performance improvements. Rajiv believes that if he asks the right questions, in fairly short order he can get the team to rediscover the optimizations he developed for Felicity's database product without actually telling them how to do it.

Which option should Rajiv take?

Kantian Evaluations

The first option is innocuous. Rajiv is sharing his expertise with the development team without disclosing any

confidential information. He is not violating the employee confidentiality and proprietary rights agreement he signed with Felicity. The moral rule, "You should share your expertise with others," can be universalized without contradiction. From a Kantian perspective, this option is morally right.

In the second option, Rajiv's will is to get the team to know what he knows without directly communicating the information. Presumably, if he asks questions in a general way, akin to a college professor posing questions for a homework assignment, the members of the team will be able to discover ways of improving the performance of the database software. However, by taking this course of action, Rajiv runs the risk of asking the team leading questions—more specifically, propositions disguised as questions that require simply a yes or no answer. Communicating confidential information, even phrased as questions, is prohibited by the confidentiality agreement Rajiv signed with Felicity. In this agreement Rajiv stated that his obligation not to reveal confidential information outside the company would continue after his employment with Felicity ended. Breaking this contract is equivalent to breaking a promise, and as we saw in Section 2.6.1, it is wrong to break a promise. From a Kantian point of view, this option is morally

acceptable only if Rajiv can get through the entire line of questioning without asking a leading question. If anywhere in the process he asks a leading question that reveals optimizations he developed at Felicity, this option would be morally wrong. Given the complexity of the system to be implemented, Rajiv's desire to help the team discover the optimizations, and the fact that he may feel pressed for time because he is helping the team in addition to his normal job responsibilities, there is a good chance he would be unable to avoid asking leading questions. From a Kantian perspective, this option is morally dubious.

Social-Contract-Theory Evaluations

Both evaluations from the perspective of social contract theory are similar to the Kantian evaluations. In the first option, Rajiv is helping the team without violating any agreements. The action is morally right.

The morality of the second option hinges on whether Rajiv can avoid communicating confidential information he acquired while at Felicity. As a condition of his employment at Felicity, Rajiv signed a confidentiality and proprietary rights agreement, and there is no overriding moral concern in this situation that would justify his breaking this agreement. If Rajiv can engage with the team and avoid asking leading

questions, his actions would be morally acceptable, but if he asks any leading questions, that would be wrong.

Act-Utilitarian Evaluations

The affected parties are Rajiv and the employees and investors of Unrelated.com. We will quantify the consequences for Rajiv by considering how each option affects his future earnings for the next five years. We will quantify the consequences for Unrelated.com by considering the effects of two different factors on the company's balance sheet over the next five years: the lost income due to the delay in the release of the product, and the expected costs (if any) associated with potential litigation.

In the first option, Rajiv sets up a "clean-room" environment for the database team to develop its optimizations. Rajiv performs a valuable service to Unrelated.com by providing the team with relevant information in the form of books, journal papers, and conference articles, as well as realistic performance targets, that enable the team to double the performance of the database system. As a result, Rajiv can reasonably expect a good raise, perhaps 10 percent, or $15,000. Over the next five years, the cumulative effect of the raise is $75,000.

Using his substantial experience and good judgment, Rajiv predicts that using the clean-room strategy to redesign the database will delay the release of the product by six months. The marketing team expects the company to reach its steady state of customers after only three years. That means a six-month delay in the release of the product will cost the company six months' revenue from its steady state of 50,000 customers over the next five years. The total loss to the company will be 50,000 customers times $10/month per customer times 6 months, or $3,000,000. Rajiv will not be working with the team developing the software, so there is no risk that he would communicate confidential information he acquired while working at Felicity. Therefore, there is no risk of litigation from Felicity, and the financial impact related to potential litigation is $0.

In the second option, Rajiv works with the team, asking the members open-ended questions that enable them to discover for themselves the database optimizations. The project is still delayed, but with Rajiv's help, he believes the team should be able to come up with the solutions more rapidly than in the previous option, and the release of the product should be delayed by only three months. The total loss of income to the

company over the next five years is 50,000 customers times $10/month per customer times 3 months, or $1,500,000.

If Rajiv chooses the second option and works directly with the team, there is a chance he may become impatient and ask the team leading questions in order to guide them to the right solution, creating the possibility of legal action by Felicity. That would only happen if Rajiv actually divulged confidential information *and* Felicity discovered what he has done *and* the legal department at Felicity chose to litigate against a small start-up company that was not a direct competitor. Using his experience and best judgment, Rajiv estimates the probability of these events occurring as 50 percent, 25 percent, and 50 percent, respectively. Altogether, the probability of litigation is $0.5 \times 0.25 \times 0.5 = 0.0625$. If Felicity did litigate, it could seek $5 million in damages from Unrelated.com, based on similar cases in the industry. The expected loss to Unrelated.com from legal action is $5,000,000 times 0.0625, or $312,500.

)

Next Rajiv calculates the consequences of the second option on his earnings over the next five years. In the unlikely event Unrelated.com must pay Felicity $5 million, he must assume he will be fired. The expected loss to his income is the probability of being fired (6.25 percent) times 5 years times

$150,000/year, or $46,875. It is much more likely (93.75 percent probability) that there will be no litigation. In that case, by demonstrating his technical prowess in the area of database design, and helping the team double the performance of the database system with only a three-month slip in the schedule, Rajiv's raise should be even larger than in the first option, where he receives a 10 percent raise. A 15 percent raise, or $22,500, yields $112,500 in additional salary over the next five years. Summing both terms, the expected consequence of the second option for Rajiv is equal to $0.9375 \times \$112{,}500 - \$46{,}875 = \$58{,}594$.

The anticipated consequences of the two courses of action are summarized in Table 4.2. Which option is preferable? As you can see, the overall financial consequences of both options are negative because in both cases the release of the product is delayed, resulting in a significant loss of revenue to Unrelated.com. However, because option 2 results in a smaller loss, Rajiv chooses it. Interestingly, Rajiv has chosen the option that has a smaller expected benefit to him personally.

Table 4.2

Affected Parties	Course of Action	
	(1) Set Up Clean Room	(2) Ask Team "Right Questions"
Rajiv	$75,000	$58,594
Unrelated.com		
Lost income due to delay	($3,000,000)	($1,500,000)

Virtue-Ethics Evaluations

Rajiv holds a position of responsibility at Unrelated.com. He is responsible for recruiting, developing, and retaining high-quality employees who can create value for the company. Through his supervision of the software development teams, he must do all he can to ensure that they produce systems that work well and contribute to the company's financial success. As an officer of the company, he must avoid doing anything that puts its future in jeopardy.

Setting up a "clean-room" development environment to help the team create a database system with higher performance is consistent with his responsibilities as a manager and company officer.

In the second option, Rajiv would become personally engaged with the team, asking the questions that would help the programmers to quickly identify crucial database optimizations. Rajiv would have to spend extra time at work, because he would also have to keep up with his other responsibilities. The willingness to work hard for the benefit

of their employees and their company is a characteristic of good managers. Sharing expertise is another laudable characteristic of good managers. However, in this option Rajiv is running the risk of putting himself in a situation where he gets impatient, reveals an optimization he developed at Felicity, and violates the confidentiality agreement he signed. That would be dishonest, and dishonesty is not a characteristic of a good employee or a good manager.

The prudent choice for Rajiv is option 1.

Conclusion

From the perspectives of Kantianism, social contract theory, and virtue ethics, the right thing for Rajiv to do is to set up a clean-room development environment for his software team and supply the team with publicly available information about database optimizations. Our act-utilitarian analysis has reached the conclusion that the other option is preferable; Rajiv should engage the members of the software development team and ask them open-ended questions until they rediscover the optimizations he discovered while working for Felicity. Note, however, that a more risk-averse act-utilitarian analysis would have assumed a higher probability of litigation from Felicity. Even a 30 percent risk

of Unrelated.com having to pay Felicity a $5 million settlement would have tilted the balance toward option 1.

4.4 Fair Use

The right given to a copyright owner to reproduce a work is a limited right. Under some circumstances, called **fair use**, it is legal to reproduce a copyrighted work without the permission of the copyright holder. Examples of fair use include citing short excerpts from copyrighted works for the purpose of teaching, scholarship, research, criticism, commentary, and news reporting.

The United States Copyright Act does not precisely list the kinds of copying that are fair use. Instead, what is considered to be fair use has been determined by the judicial system. The courts have relied on Section 107 of the Copyright Act, which lists four factors that need to be considered [40]:

1. *What is the purpose and character of the use?*

   The purposes of criticism, commentary, news reporting, teaching, scholarship, and research are more likely to be permissible than a commercial purpose.

   When judging the character of the use, the most important consideration is the extent to which the author has transformed the original copyrighted work.

The more the author has added new expression or meaning to the work, the more likely the work will be judged to be fair use [**41**].

2. *What is the nature of the work being copied?*

   Use of nonfiction is more likely to be permissible than use of fiction. Published works are preferred over unpublished works.

3. *How much of the copyrighted work is being used?*

   Brief excerpts are more likely to be permissible than entire chapters.

4. *How will this use affect the market for the copyrighted work?*

   Use of out-of-print material is more likely to be permissible than use of a readily available work. A spontaneously chosen selection is better than an assigned reading in the course syllabus.

Let's consider two scenarios in which copyrighted works are duplicated and determine if they made fair use of the material. These scenarios are closely modeled after situations presented on the Web site of CETUS, the Consortium for

Educational Technology in University Systems (www.cetus.org).

Fair Use Example #1

A professor puts a few journal articles on reserve in the library and makes them assigned reading for the class. Some students in the class complain that they cannot get access to the articles because other students always seem to have them checked out. The professor scans them and posts them on their Web site. The professor gives the students in the class the password they need to access the articles.

The first factor to consider is the purpose of the use. In this case the purpose is strictly educational. This factor weighs in favor of fair use.

The second factor is the nature of the work being copied. The journal articles are nonfiction. Again this weighs in favor of

fair use.

The third factor is the amount of material being copied. The fact that the professor is copying entire articles rather than brief excerpts weighs against a ruling of fair use.

The fourth factor is the effect the copying will have on the market for journal sales. If the journal issues containing these articles are no longer for sale, then the professor's actions cannot affect the market. The professor took care to prevent people outside the class from accessing the articles. Overall, this factor appears to weigh in favor of fair use.

Three of the four factors weigh in favor of fair use. The professor's actions probably constitute fair use of the copyrighted material.

Fair Use Example #2

An art professor takes photographs of a number of paintings reproduced in a book about Renaissance artists. They incorporate the photos into PowerPoint lectures for their class.

The first factor to consider is the purpose of the copying. The professor's purpose is strictly educational. Hence the first factor weighs in favor of fair use.

The second factor is the type of material being copied. The material is art. Hence this factor weighs against a ruling of fair use.

The third factor is the amount of material copied. In this case the professor is displaying copies of the paintings in their entirety. Fair use almost never allows a work to be copied in its entirety. Note that even if the original painting is in the public domain, the photograph of the painting appearing in the art book is probably copyrighted.

The final factor is the effect the copying will have on the market. The determination of this factor would depend on

how many images the professor took from any one book and whether the publisher is in the business of selling slides of individual images appearing in its book.

Overall, this professor's actions are less likely to be considered fair use than the actions of the professor in the first example.

4.4.1 *Sony v. Universal City Studios*

In 1975 Sony introduced its Betamax system, the first consumer VCR. People used these systems to record television shows for viewing later, a practice called **time shifting**. Some customers recorded entire movies onto videotape.

A year later, Universal City Studios and Walt Disney Productions sued Sony, saying it was responsible for copyright infringements performed by those who had purchased VCRs. The movie studios sought monetary damages from Sony and an injunction against the manufacturing and marketing of VCRs. The legal battle went all the way to the US Supreme Court. The Supreme Court evaluated the case in light of the four fair-use factors.

The first factor is the intended purpose of the copying. Since the purpose is private, not commercial, time shifting should be seen as fair use with respect to the first factor.

The second factor is the nature of the copied work. Consumers who are time shifting are copying creative work. This would tend to weigh against a ruling of fair use.

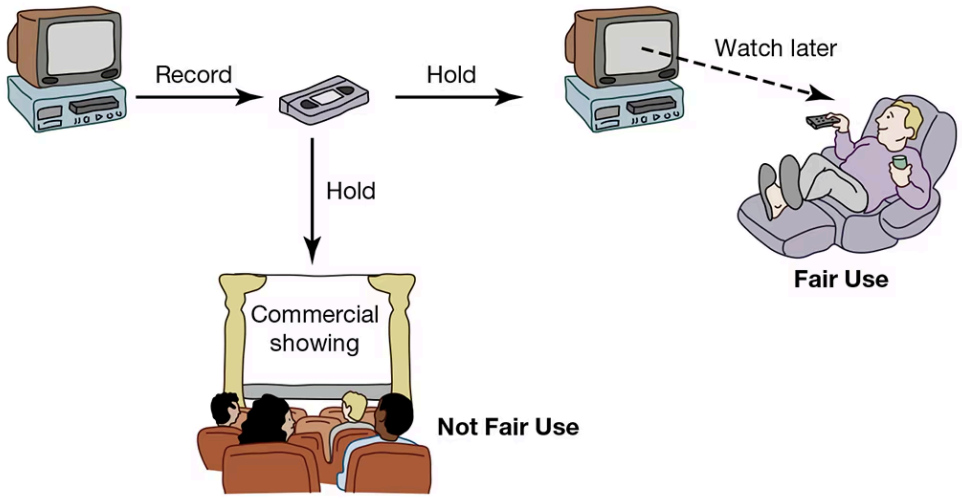
The third factor is the amount of material copied. Since a consumer copies the entire work, this weighs against a ruling of fair use.

The final factor is the effect time shifting will have on the market for the work. The Court determined that the studios were unable to demonstrate that time shifting had eroded the commercial value of their copyrights. The movie studios receive large fees from television stations in return for allowing their movies to be broadcast. Television stations can pay these large fees to the studios because they receive income from advertisers. Advertising rates depend on the size of the audience; the larger the audience, the more a television station can charge an advertiser to broadcast a commercial. Time shifting allows people who would not ordinarily be able to watch a show to view it later. Hence it can be argued that VCRs actually increase the size of the audience, and since

audience size determines the fees studios receive to have their movies broadcast on television, it is not at all clear whether the copying of these programs harms the studios.

The Supreme Court ruled, in a 5–4 decision, that time shifting television programs is a fair use of the copyrighted materials. It said that the private, noncommercial home use of recordings of broadcast material was a legitimate fair use of copyrighted works (Figure 4.5). Importantly, the Court also noted that the Sony Betamax VCR could be used to copy both copyrighted and noncopyrighted material, and that Sony should not be held accountable if some of the people who buy a VCR choose to use it to infringe on copyrights [42].

Figure 4.5



The Supreme Court ruled that videotaping television broadcasts for private viewing at a later time is fair use of the copyrighted material. This practice is called time shifting. Using videotaped material for a commercial purpose is not considered fair use.

4.4.2 Audio Home Recording Act of 1992

The Audio Home Recording Act represents a compromise between the desires of the recording industry, the electronics industry, and consumers. The Act protects the right of consumers to make copies of analog or digital recordings for personal, noncommercial use. For example, a consumer may copy a recording to put in another music player, to give to another family member, or to use as a backup.

To reduce the problem of unauthorized copying, the Audio Home Recording Act requires manufacturers of digital audio recorders to incorporate the Serial Copyright Management System (SCMS). The SCMS allows a consumer to make a digital copy from the original recording, but it prevents someone from making a copy of the copy.

To compensate artists and recording companies for the loss of sales due to copying, the Audio Home Recording Act requires a royalty to be paid on the sale of all digital audio-recording devices and blank digital audio-recording media. The royalties are divided among songwriters, music publishers, musicians, and recording companies, based on the

popularity of their music. As it turns out, these royalty payments have never been a significant source of income for any of these groups.

4.4.3 *RIAA v. Diamond Multimedia*

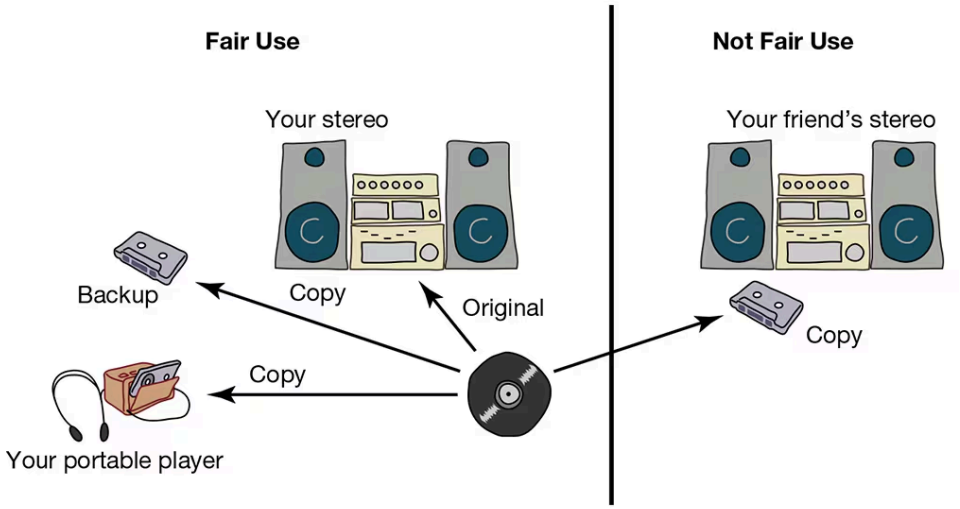
A **compression algorithm** reduces the number of bits needed to store a picture or sound. The most popular compression algorithm for music is MP3, which was developed by a team of European scientists. An MP3 music file is typically less than 10 percent the size of the original file, and it is difficult to hear the difference between the original and the compressed versions. The availability of MP3 encoders and decoders in the mid-1990s helped speed the development of portable music players.

Diamond Multimedia Systems introduced the Rio MP3 portable music player in 1998. About the size of a pack of cigarettes, the Rio stored an hour of digitized music. The Recording Industry Association of America (RIAA) asked for an injunction preventing Diamond Multimedia from manufacturing and distributing the Rio. The RIAA alleged that the Rio did not meet the requirements of the Audio Home Recording Act of 1992 because it did not employ the

Serial Copyright Management System to prevent unauthorized copying of copyrighted material.

The US Court of Appeals, Ninth Circuit, upheld the ruling of a lower court that the Rio was not a digital audio-recording device as defined by the Audio Home Recording Act. It denied the injunction on these technical grounds. In addition, the Court affirmed that **space shifting**, or copying a recording in order to make it portable, is fair use and entirely consistent with copyright law (Figure 4.6).

Figure 4.6



Space shifting is the creation of a copy for backup purposes or for use in a portable device, and it is considered fair use. Making a copy for a friend is not considered fair use.

4.4.4 *Kelly v. Arriba Soft*

Leslie Kelly was a photographer who maintained a Web site containing many of his copyrighted photos. Arriba Soft

Corporation created an Internet-based search engine that responded to user queries by displaying thumbnail images. Arriba Soft created the thumbnail images by copying images from other Web sites. When Kelly discovered that the Arriba Soft search engine was displaying thumbnail images of his photographs, he sued Arriba Soft for copyright infringement.

The US Court of Appeals, Ninth Circuit, upheld the ruling of a lower court that Arriba Soft's use of the images was a fair use of the work [**43**]. Two factors heavily favored Arriba Soft's claim of fair use. First, the character of Arriba Soft's use of the images was "significantly transformative" [**43**]. Kelly's original images were artistic creations designed to provide the viewer with an aesthetic experience. Arriba Soft's use of the thumbnails was to create a searchable index that would make it easier for people to find images on the Internet. The thumbnail images had such low resolution that enlarging them resulted in a blurry image with little aesthetic appeal. Second, Arriba Soft's use of Kelly's images did not harm the value of the original images or the market for these images. If anything, the search engine's display of Kelly's images "would guide users to Kelly's Web site rather than away from it," increasing the demand for his photographs [**43**].

4.4.5 *Authors Guild v. Google*

In December 2004, Google announced a plan to scan millions of books held by Harvard University, the University of Michigan, the New York Public Library, Oxford University, and Stanford University, creating a database containing the words in all of these books [**44**]. This database is much more powerful than traditional library card catalogs because it allows users to search for words or phrases appearing anywhere in the cataloged books. The system responds to a user query by returning the books that match the query most closely. If the book is in the public domain, the user can view and download a PDF file containing the scanned images of the book's pages. If the book is still under copyright, the user can see a few sentences from the book that show the search term in context, and the search engine provides links to libraries holding the book and online bookstores selling the book.

In September 2005, the Authors Guild filed a lawsuit in the US District Court for the Southern District of New York, claiming that "by reproducing for itself a copy of those works that are not in the public domain, Google is engaging

in massive copyright infringement" [**45**]. A month later a group of five major publishers sued Google for copyright infringement. The publishers claimed that Google was infringing their rights under the Copyright Act because Google's intent was "purely commercial," and in order to create its database, Google was systematically copying entire books still protected by copyright [**46**]. Google's defense was that its book-scanning project should be considered fair use under Section 107 of the Copyright Act.

After a long and complicated legal battle, in November 2013 Judge Denny Chin found in favor of Google and dismissed the lawsuit. Using the four factors listed in Section 107 of the Copyright Act as his guide, he explained why he determined that Google Books was a fair use of copyrighted books:

- The first factor concerns the purpose and character of the use. Chin noted that the purpose of the Google Books project is to create a massive index from the words appearing in the books, and the character of "Google's use of the copyrighted works is highly transformative" [**47**, p. 19]. The index Google has created is a powerful tool for librarians, scholars, and researchers. The judge cited the precedent of *Kelly v. Arriba Soft Corporation*. Google's display of small

portions of the text of a book is similar to Arriba Soft's display of thumbnail images of photographs. The Google Books project has also been transformative by making possible entirely new kinds of research, such as exploring how the usage of words changes over time. Chin concluded, "the first factor strongly favors a finding of fair use" [47, p. 22].

- The second factor is the nature of the work being copied. Most of the books Google is scanning are nonfiction, and all of the scanned books are published. These factors "favor a finding of fair use" [47, p. 23].
- The third factor has to do with how much of the copyrighted work is being used. In order to index a book, Google must scan the entire book. Even though Google limits the amount of text displayed in response to a query, this factor "weighs slightly against a finding of fair use" [47, p. 24].
- The fourth factor to consider is the effect of Google's use of the copyrighted work on the market for that work. Chin rejected the plaintiffs' argument that the Google Books project would reduce book sales, determining that the Google Books project is actually stimulating book sales by helping people discover

> books. The judge concluded the fourth factor "weighs strongly in favor of a finding of fair use" [47, p. 25].

The Electronic Frontier Foundation praised the ruling, calling it "a good day for fair use and sane copyright law" [48], but the plaintiffs did not give up. The Authors Guild appealed the ruling to the US Court of Appeals for the Second Circuit, which unanimously affirmed the judgment in favor of Google in October 2015 [49]. The Authors Guild then filed a petition for writ of certiorari with the US Supreme Court, but its petititon was denied in April 2016, leaving intact the decision of the US Court of Appeals for the Second Circuit [50].

4.4.6 Mashups

In music, a **mashup** is a composition that incorporates elements taken from preexisting songs. In the simplest form of a mashup, called A vs. B, an artist overlays the instrumental track from one song with the vocal track from another song. An example of an A vs. B mashup is "A Stroke of Geni-Us" by Freelance Hellraiser, which overlays the instrumental track from "Hard to Explain" by the Strokes with Christina Aguilera's voice track from "Genie in a Bottle." In a sophisticated mashup, called an audio collage, the artist creates a new composition from dozens of audio

fragments. DJ Danger Mouse created an audio collage consisting of vocal samples from Jay Z's *The Black Album* and instrumental samples from the Beatles' *White Album*, creating completely new songs that he issued as *The Grey Album* (naturally).

After Danger Mouse distributed 3,000 promotional copies of *The Grey Album* in 2004, he received a cease-and-desist order from EMI, the publisher owning the copyright to the Beatles' works. Danger Mouse complied with the order and never sold the album, but in an act of civil disobedience others made copies available over the Internet.

Is a mashup an example of fair use? Courts have not yet ruled on this issue, but Elina Lae has argued that the answer should depend on the type of mashup. In Lae's view, an audio collage is highly transformative and should receive protection under the fair-use provision of the Copyright Act. In contrast, an artist creating an A vs. B mashup is not creating a transformative work and should be required to obtain licenses from the owners of the copyrighted sources. Regardless of whether the artist is creating an audio collage or an A vs. B, if the purpose of the mashup is "criticism, satire, or parody," the mashup should be entitled to fair use protection, suggests Lae [**41**].

4.5 Digital Media

CDs and DVDs store sounds and images in digital form. When information is stored digitally, anyone with the right equipment can make perfect copies, making copyright infringement easier.

The increase in the number of people with broadband Internet connections has stimulated digital copying. The number of illegal downloads soared when more people gained broadband access to the Internet [**51**]. As a result, the music industry has lost sales. Total revenue from music sales and licensing in the United States dropped from $14.6 billion in 1999 to $6.3 billion in 2009 [**52**].

Governments and recording companies have responded to the threat of illegal copying of copyrighted materials by introducing new legal and technological restrictions on copying. Sometimes that makes it impossible for consumers to make copies even for purposes that are considered fair use, such as making a backup.

4.5.1 Digital Rights Management

Digital rights management (DRM) refers to any of a variety of actions owners of intellectual property may take to protect their rights. As Christopher May puts it, "All DRM technologies are aimed at tracking and controlling the use of content once it has entered the market" [53]. DRM technologies may be incorporated into a computer's operating system, a program, or a piece of hardware.

One approach to DRM is to encrypt the digital content so that only authorized users can access it. Another approach is to place a digital mark on the content so that a device accessing the content can identify the content as copy protected.

4.5.2 Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA), passed by Congress in 1998, was the first major revision of US copyright law since 1976. The primary purpose of the DMCA was to bring the United States into compliance with

international copyright agreements it had signed [40]. Provisions in the DMCA significantly curtail fair use of copyrighted material. The DMCA makes it illegal for consumers to circumvent encryption schemes placed on digital media, and it is illegal to sell (or even discuss online) a software program designed to circumvent copy controls [54].

Online service providers that misuse copyrighted materials face severe penalties [54]. That means, for example, a university that knows students are exchanging MP3 files on the campus network and does nothing to stop them can be sued [55].

The DMCA requires Internet radio stations to make royalty payments to the copyright holders of music they broadcast. The rates paid by Internet radio stations are set by the Copyright Royalty Board.

4.5.3 Secure Digital Music Initiative

The Secure Digital Music Initiative (SDMI) was an effort to create copy-protected CDs and secure digital music downloads that would play only on SDMI-compliant devices. About 200 entertainment and technology companies joined

the consortium, which worked for three years to develop "digital watermarks" that would make unauthorized copying of audio files impossible. The SDMI was unsuccessful for three reasons. First, before any copy-protection technologies could be put in place, the number of music files being copied on the Internet mushroomed. Second, some of the sponsors of the SDMI—consumer electronics companies—started making a lot of money selling devices that became more attractive to customers as access to free MP3 files got easier. Their sales could be hurt by restrictions on copying. Third, the digital watermarking scheme was cracked [**56**]. Here's how that happened.

In September 2000, SDMI issued a "Hack SDMI" challenge. It released some digitally watermarked audio files and offered a $10,000 prize to the first person to crack them. Princeton computer science professor Edward Felten and eight colleagues picked up the gauntlet. Three weeks later the team had successfully read the audio files. The team declined to accept the cash prize. Instead, they wrote a paper describing how they broke the encryption scheme. They prepared to present the paper at the Fourth Annual Information Hiding Workshop at Carnegie Mellon University in April 2001 [**57**]. At this point, the Recording Industry Association of America sent Dr. Felten a letter warning him that if he disclosed any

of the information he learned by participating in the challenge, he and his team could be sued for violating the Digital Millenium Copyright Act [58]. Fearing litigation, Dr. Felten agreed to withdraw the paper from the conference. However, that did not prevent the information from being leaked. Even before the conference, copies of the research paper and the letter from the RIAA were placed on a freedom-of-speech Web site [58]. Four months later Felten's group published the paper [59].

4.5.4 Sony BMG Music Entertainment Rootkit

In the summer and fall of 2005, Sony BMG Music Entertainment shipped millions of audio CDs with Extended Copy Protection, a DRM system. Extended Copy Protection prevented users from ripping audio tracks into MP3 format or making more than three backup copies of the CD. It also monitored the user's listening habits and reported back to Sony via the Internet. Extended Copy Protection did this by secretly installing a rootkit on Windows computers when the CD was played for the first time. A **rootkit** is a way of hiding files and processes from users; rootkits are commonly associated with computer hackers. The installation of the

rootkit also compromised the security of the user's computer, making it vulnerable to "Trojan horse" programs (see Section 7.3.8) [**60**].

A computer expert discovered the Sony rootkit on his computer and publicized its existence, resulting in a huge public outcry and a class action lawsuit. Without admitting any wrongdoing, Sony BMG agreed to do the following [**61**]:

- Cease production of CDs with Extended Copy Protection
- Provide financial incentives to retailers to return unsold audio CDs with Extended Copy Protection
- Make freely available the software patch needed to uninstall the rootkit
- Allow customers to exchange CDs with Extended Copy Protection for identical CDs with no DRM
- Give consumers $7.50 or three free album downloads for every CD with Extended Copy Protection they exchange

4.5.5 Criticisms of Digital Rights Management

The introduction of DRM technologies has been controversial. Here are some criticisms that have been raised against DRM.

)

Many experts suggest that any technological “fix” to the problem of copyright abuse is bound to fail. All prior attempts to create encryption or anticopying schemes have been abandoned or circumvented.

Others argue that DRM undermines the well established principle of fair use. Under DRM, a consumer may not be able to make a private copy of a DRM-protected work without making an extra payment, even if they have the right to do so under traditional fair-use standards. Selena Kim writes:

> **In the analogue world, people go ahead and use the work if they believe themselves entitled to do so. It is only if users are sued for infringement that they invoke the relevant copyright exceptions as defence. In a digital world encapsulated by access control and embedded with copy control, a potential user of a work may have**

> **to ask for permission twice: once to access a work, and again to copy an excerpt. The exception to copyright is not being put forward as a defence; it is put forward to show entitlement to use the work [62, p. 112].**

DRM restrictions sometimes prevent libraries from reformatting materials to make them more accessible to persons with disabilities. In addition, DRM protections, unlike copyrights, never expire [63].

Finally, some DRM schemes prevent people from anonymously accessing content. Microsoft's Windows Media Player has an embedded globally unique identifier (GUID). The Media Player keeps track of all the content the user views. When the Media Player contacts Microsoft's central server to obtain titles, it can upload information about the user's viewing habits.

4.5.6 Online Music Stores Drop Digital Rights Management

When Apple began selling music through the iTunes Music Store in 2003, all the songs were protected with a DRM scheme called FairPlay. FairPlay blocked users from freely exchanging music they had purchased by preventing songs from being played on more than five computers or being copied onto CDs more than seven times. FairPlay had two other "features" that were strong incentives for consumers to stick with the Apple brand: music purchased from the iTunes store couldn't be played on portable devices other than the Apple iPod, and DRM-protected music purchased from other online retailers couldn't be played on the iPod [**64**].

Consumers complained about the restrictions associated with DRM, and eventually music retailers responded. In 2007 EMI announced it would begin offering all its songs without DRM through the iTunes store for $1.29, 30 cents more than the previous price [**65**]. A year later, Amazon became the first online music store to reach an agreement with all four major labels to sell music free of DRM restrictions [**66**]. Apple followed suit in 2009 with an announcement that it, too, had reached an agreement with all the major music labels to sell music without DRM restrictions [**67**].

4.5.7 Microsoft Xbox One

In June 2013, Microsoft announced that it was creating a cloud-based gaming experience to coincide with the launch of Xbox One. In the new environment, people would be able to play their games from any Xbox One without the disc being in the tray, and every Xbox One would automatically be kept current with the latest system and application updates [68].

Consumers soon learned about the restrictions accompanying these benefits, and their reactions were overwhelmingly negative. Three features of the proposed licensing arrangement were particularly controversial: a disc owner would be allowed to share a disc only once, freedom to sell discs and buy secondhand titles was restricted, and Xbox consoles would have to check in online every 24 hours to ensure that the authorized software was up-to-date and that there was no unauthorized software [69]. In the midst of the controversy, Amazon ran a Facebook poll to see which new gaming console consumers were more interested in purchasing: the Microsoft Xbox One or the Sony PlayStation 4. The PlayStation 4 was capturing 95 percent of the votes when Amazon decided to shut down the poll early [70].

Microsoft did not waste time changing course. Thanking consumers for their "assistance in helping us to reshape the future of Xbox One," Microsoft's Don Mattrick announced

that the controversial features of the licensing agreement were being dropped [71]. In particular, he indicated consumers would be able to play Xbox One games without being connected to the Internet, the Xbox One would not need to connect to the Internet once every 24 hours, and consumers would be free to lend, rent, or sell their discs. This reversal also meant that people would no longer have the ability to play their games from any Xbox One console without the disc being in the tray.

4.6 Peer-to-Peer Networks and Cyberlockers

On the Internet, the term **peer-to-peer** refers to a transient network allowing computers running the same networking program to connect with each other and access files stored on each other's hard drives. Peer-to-peer networks stimulate the exchange of data in three ways. First, they give each user access to data stored in many other computers. Second, they support simultaneous file transfers among arbitrary pairs of computers. Third, they allow users to identify those systems that will be able to deliver the desired data more rapidly, perhaps because they have a faster Internet connection or are fewer routing hops away.

Cyberlockers (also called **file-hosting services** or cloud storage services) are Internet-based file-sharing services that allow users to upload password-protected files. Users can give other people access to the files they have uploaded by sharing passwords. People who wish to collaborate on a

project often find sharing large files through cyberlockers more convenient than sending them back and forth as attachments to email messages. However, cyberlockers also make it easy for people to share copyrighted material, such as songs and movies. In addition, cyberlocker use is much more difficult for government officials to track than peer-to-peer file sharing.

4.6.1 RIAA Lawsuits Against Napster, Grokster, and Kazaa

Napster, Grokster, and Kazaa were peer-to-peer networks that facilitated the exchange of music files. Napster used a central computer to maintain a global index of all files available for sharing. In contrast, Grokster and Kazaa used a software technology called FastTrack to distribute the index of available files among a large number of computers.

In December 1999, the RIAA sued Napster for copyright infringement, asking for damages of $100,000 each time a Napster user copied a copyrighted song. In June 2000, the RIAA asked for a preliminary injunction to block Napster from trading any copyrighted content from major record

labels. In February 2001, a federal appeals court ruled that Napster must stop its users from trading copyrighted material. Napster put in place file-filtering software that was 99 percent effective in blocking the transfer of copyrighted material. In June 2001, a district court judge ruled that unless Napster could block 100 percent of attempted transfers of copyrighted material, it must disable file transfers. This court order effectively killed Napster, which went offline in July 2001 and officially shut down in September 2002 [**72**, **73**, **74**]. (The following year Napster reemerged as an online subscription music service and music store.)

In April 2003, the RIAA warned Grokster and Kazaa users that they could face legal penalties for swapping files containing copyrighted music. The message read, in part:

> **It appears that you are offering copyrighted music to others from your computer . . . . When you break the law, you risk legal penalties. There is a simple way to avoid that risk: DON'T STEAL MUSIC, either by offering it to others to copy or downloading it on a "file-sharing" system like this. When you offer music on these systems, you are not anonymous and you can easily be identified.** [75]

The RIAA identified the IP addresses of the most active Kazaa supernodes, leading it to the ISPs of users who had stored large numbers of copyrighted files on their computers. Under the terms of the Digital Millennium Copyright Act, the RIAA subpoenaed Verizon, asking it to identify the names of customers suspected of running these Kazaa supernodes. Verizon resisted responding to the subpoenas, claiming that responding to the subpoenas would violate the privacy of its customers. In June 2003, a judge in Washington, DC, ruled that Verizon had to release the names of the customers [**76**].

In September 2003, the RIAA sued 261 individuals for distributing copyrighted music over the Internet [77]. A month later the RIAA sent letters to 204 people who had downloaded at least 1,000 music files, giving them an opportunity to settle before being sued by the RIAA [**78**].

In December 2003, the RIAA suffered a setback when the US Court of Appeals for the District of Columbia Circuit ruled that Verizon did not have to respond to the subpoenas of the RIAA and identify its customers [**79**]. Still, there is some evidence the RIAA lawsuits reduced illegal file swapping across the Internet. A survey from Com-Score reported activity on Kazaa declined by 15 percent between November 2002 and November 2003 [**80**]. The Pew Internet &

American Life Project reported that the percentage of Internet users who said they download music dropped from 32 percent in October 2002 to 22 percent in January 2005, and more than half of the January 2005 downloaders said that they purchased their music from an online service, such as iTunes. However, the report cautioned that because of the stigma associated with illegal downloading, fewer people may have been willing to admit they do it. Interestingly, about half of music downloaders said they had gotten music from email, instant messages, or someone else's MP3 player or iPod [**81**].

The RIAA's campaign to impose severe penalties on file sharers has been successful in the courtroom, but huge jury judgments against file sharers have been overruled by judges. In June 2009, a federal jury in Minnesota ordered Jammie Thomas-Rasset, a single mother of four, to pay $1.92 million —$80,000 a song—for violating the copyrights of 24 songs [**82**]. (The RIAA accused her of making 1,700 songs available on Kazaa, but they only tried to prove 24 copyright infringements.) In July 2011, Judge Michael Davis reduced the damage award against Thomas-Rasset to $54,000. Judge Davis called the original award "appalling," and said it was "so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable" [**83**].

Another verdict went the RIAA's way in July 2009. The RIAA had accused Joel Tenenbaum of copyright infringement for using Kazaa to share 31 music files. The jury awarded the music companies $675,000, or $22,500 per song [84]. In July 2010, Judge Nancy Gertner reduced the jury's award to $67,500. In her ruling, Judge Gertner wrote: "There is substantial evidence indicating that Congress did not contemplate that the Copyright Act's broad statutory damages provision would be applied to college students like Tenenbaum who file-shared without any pecuniary gain. . . . There is no question that this reduced award is still severe, even harsh. It not only adequately compensates the plaintiffs for the relatively minor harm that Tenenbaum caused them; it sends a strong message that those who exploit peer-to-peer networks to unlawfully download and distribute copyrighted works run the risk of incurring substantial damages awards" [85, p. 3].

During these trials, the RIAA did not prove that people had actually downloaded songs from the defendants' computers. Instead, they contended that simply making the music files available to others was a violation of copyright law. In other words, making it possible for someone to download a music file from you means you've violated copyright law, even if no one ever does it. In April 2008, a federal court judge in New

York agreed with the position of the RIAA, but judges in Massachusetts and Arizona reached the opposite conclusion, holding that simply making music files available for copying is not copyright infringement [86, 87, 88].

4.6.2 *MGM v. Grokster*

A group of movie studios, recording companies, music publishers, and songwriters sued Grokster and StreamCast for the copyright infringements of their users. The plaintiffs (henceforth referred to as MGM) sought damages and an injunction against the defendants.

During the discovery phase of the litigation, the following facts were revealed:

- The defendants' networks were used to transfer billions of files every month.
- About 90 percent of the files available on Grokster's FastTrack network were copyrighted.
- Grokster and StreamCast promoted their networks to investors and potential customers as replacements for Napster.

- An internal StreamCast document revealed that StreamCast's executives wanted to have more copyrighted songs available on their network than on competing networks.
- Grokster sent its users a newsletter touting its ability to deliver popular copyrighted songs.
- Grokster and StreamCast provided technical support to users who were having difficulty locating or playing copyrighted content.

A US District Court granted Grokster and StreamCast a summary judgment; that is, it made its decision without a trial based on the facts and evidence collected. According to the judge, "The defendants distribute and support software, the users of which can and do choose to employ it for both lawful and unlawful ends. Grokster and StreamCast are not significantly different from companies that sell home video recorders or copy machines, both of which can be and are used to infringe copyrights" [89]. The judge referred to *Sony v. Universal City Studios*, the Supreme Court's 1984 ruling on the legality of Sony's Betamax VCR. MGM appealed to the US Court of Appeals for the Ninth Circuit, which upheld the ruling.

After another appeal, the US Supreme Court unanimously reversed the decision of the lower courts in June 2005. Justice Souter wrote: “The question is under what circumstances the distributor of a product capable of both lawful and unlawful use is liable for acts of copyright infringement by third parties using the software. We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties” [90].

The Supreme Court made clear it was not reversing the Sony Betamax decision. Instead, it ruled that the “safe harbor” provided to Sony did not apply to Grokster and StreamCast. The Sony Betamax VCR was primarily used for time-shifting television shows, which the Court found to be a fair use. There was no evidence Sony had done anything to increase sales of its VCRs by promoting illegal uses. Therefore, Sony could not be found liable simply for selling VCRs.

The situation for Grokster and StreamCast was quite different. Both companies gave away their software but made money by streaming advertisements to users. Advertising rates are higher when the number of users is greater. Hence both companies wanted to increase their user base. They

realized the way to do this was to make sure their networks had the content people were interested in downloading. The opinion notes dryly, “Users seeking Top 40 songs, for example, or the latest release by Modest Mouse, are certain to be far more numerous than those seeking a free Decameron, and Grokster and StreamCast translated that demand into dollars. . . . The unlawful objective is unmistakable” [**90**].

According to the Supreme Court, the Ninth Circuit Court of Appeals erred when it cited *Sony v. Universal City Studios*. The more relevant precedent was *Gershwin Publishing Corporation v. Columbia Artists Management, Inc*. The Supreme Court remanded the case to the Court of Appeals, suggesting that a summary judgment in favor of MGM would be in order. Grokster shut down its peer-to-peer network in November 2005 and paid $50 million to “movie studios, record labels and music publishers” [**91**].

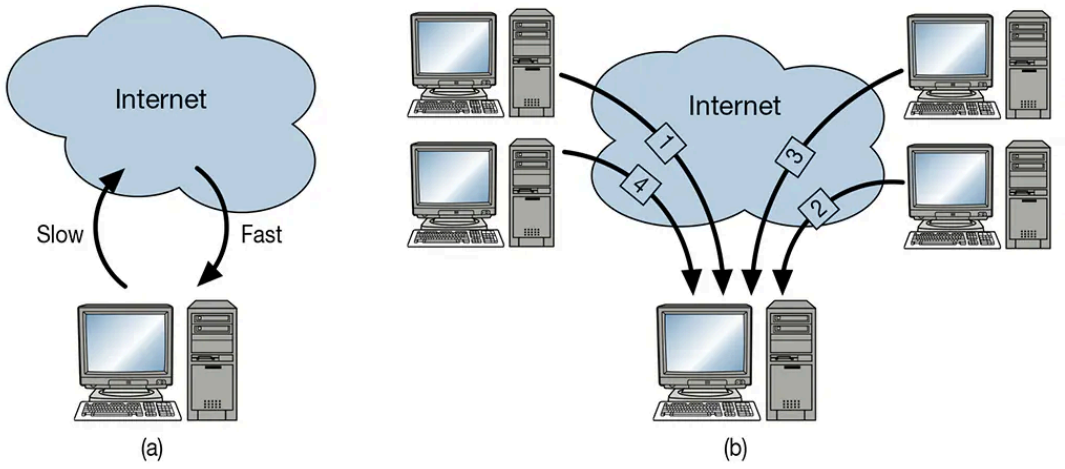
4.6.3 BitTorrent

For a computer with a broadband connection to the Internet, downloading a file from the network is about 10 times faster than uploading a file to the network. A problem with FastTrack and some other peer-to-peer networking protocols

is that when one peer computer shares a file with another peer computer, the file is transferred at the slower upload speed rather than the faster download speed. To solve the problem caused by slower uploading speed, Bram Cohen developed BitTorrent [92].

BitTorrent divides a file into pieces about a quarter-megabyte in length. Different pieces of a file can be downloaded simultaneously from different computers, avoiding the bottleneck that occurs when the entire file is uploaded from a single computer (Figure 4.7). As soon as a user has a piece of a file, the user can share this piece with other users. Since BitTorrent gives a priority for downloads to those users who allow uploading from their machines, users tend to be generous. As a result, downloading speeds increase as more peers get a copy of the file. Put another way, downloading speeds increase with the popularity of a title.

Figure 4.7



(a) Broadband Internet connections provide higher speeds for downloading than for uploading. (b) BitTorrent reduces downloading time by enabling a computer to download different pieces of a file simultaneously from many different peers.

With its markedly higher downloading rates, BitTorrent has made practical the exchange of files hundreds of megabytes long. People are using BitTorrent to download copies of computer programs, television shows, and movies. Linspire, a Linux operating system developer, reduces demand on its servers (and saves money) by using BitTorrent to distribute its software [**93**]. BitTorrent was also the vehicle by which *Revenge of the Sith* became available on the Internet before it appeared in movie theaters [**94**].

4.6.4 Legal Action Against the Pirate Bay

The Pirate Bay, based in Stockholm, Sweden, is one of the biggest file-sharing Web sites in the world, with an estimated 25 million users [**95**]. People use the Pirate Bay to search for songs, movies, TV shows, or computer programs they can download for free. These items of intellectual property are broken into BitTorrent fragments stored in thousands of different computers scattered across the globe. Established in 2003, the Pirate Bay has been called “the most visible

member of a burgeoning international anti-copyright—or pro-piracy—movement" [96].

The movie industry pressured the Swedish government to do something about the Pirate Bay, and in 2006 Swedish police raided its offices and confiscated 186 servers, but the site was offline for only three days [96, 97]. After the site was reactivated, the number of people accessing it increased significantly, perhaps because of the international publicity the Pirate Bay received as a result of the raid [96].

In 2008 the International Federation of the Phonographic Industry sued four individuals connected with the Pirate Bay for making available 33 copyrighted works: twenty songs, nine films, and four computer games [95]. The defendants argued that the Pirate Bay is simply a search engine and does not host any copyrighted content [98]. In April 2009, a District Court in Stockholm found Carl Lundström, Fredrik Neij, Peter Sunde, and Gottfrid Svartholm Warg guilty of aiding and abetting copyright infringement. All four were sentenced to one year in prison, and altogether were fined 30 million Swedish kronor (about $3.6 million). In November 2010, an appeals court in Sweden upheld the convictions but shortened the sentences and increased the fine to 46 million kronor ($6.5 million) [99].

Meanwhile, the Pirate Bay Web site is still operational and enormously popular. In many countries the Pirate Bay's official URL is blocked by Internet service providers. People in these countries are still able to access the Pirate Bay by connecting to one of more than 150 proxy sites hosted in countries that do not block access to the Pirate Bay.

4.6.5 PRO-IP Act

In 2008 the US Congress passed the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act. The PRO-IP Act gives federal law-enforcement agencies the authority to seize the domain names of Web sites that are allegedly facilitating copyright infringement or trafficking in counterfeit goods.

In June 2010, the US Department of Immigration and Customs Enforcement launched Operation In Our Sites, seizing the domain names of 10 Web sites that were making available first-run movies "often within hours of their theatrical release" [**100**]. Over the next year and a half, several hundred more domain names were seized, including sites that were streaming live broadcasts of the National Football League, the National Basketball Association, the

National Hockey League, World Wrestling Entertainment, and the Ultimate Fighting Championship [**101**].

4.6.6 Megaupload Shutdown

Megaupload Limited, based in Hong Kong, was a prominent cyberlocker. It had more than 180 million registered users, and at one point it was the world's 13th most popular Web site, accounting for "approximately four percent of the total traffic on the Internet" [**102**]. A substantial percentage of the network traffic to and from the cyberlocker was associated with the sharing of copyrighted movies, television programs, songs, and computer games. The founder of Megaupload, Kim Dotcom, lived in Auckland, New Zealand.

In January 2012, the FBI worked with police in New Zealand and Hong Kong to shut down the Megaupload cyberlocker and arrest Kim Dotcom and three associates for violating the PRO-IP Act [**103**]. According to the grand jury indictment, Kim Dotcom and his codefendants were part of "a worldwide criminal organization whose members engaged in criminal copyright infringement and money laundering on a massive scale with estimated harm to copyright holders well in excess of $500,000,000 and reported income in excess of

$175,000,000" [**102**]. The indictment claimed that the defendants had paid millions of dollars to premium subscribers for uploading popular copyrighted works to the cyberlocker, as a way of increasing the number of paid subscribers.

Other cyberlockers responded quickly to the news. A few days after the shutdown of Megaupload, FileSonic posted an announcement on its Web site, stating that it had disabled all file-sharing functionality [**104**]. The FileServe site posted a similar message [**105**].

4.6.7 Legal Online Access to Entertainment

The widespread piracy of music, television shows, and movies on the Internet has put pressure on companies selling these products to make "doing the right thing"—obtaining a legal copy—as easy as "doing the wrong thing" [**106**]. Industry has risen to the challenge.

A good example is the continued evolution of online music services. As we saw in Section 4.5.6, when Apple launched the iTunes Music Store, it included a digital-rights management system called FairPlay with the songs that were

downloaded. Consumers were unhappy with the FairPlay restrictions. Meanwhile, Amazon reached an agreement with all four major labels to sell music without digital-rights management restrictions. Responding to these consumer and competitive pressures, Apple dropped FairPlay and began selling music free of digital-rights management.

Now, more than a decade later, consumers have shifted from music ownership toward anytime-anywhere access offered by music streaming services [**107**]. Globally, there are more than 400 licensed music services, including Spotify, Deezer, Pandora, and Apple Music. These providers offer two streaming-service models. In the ad-supported model, listeners can have music and advertisements streamed to their devices for free; the services earn income and pay royalties to artists from advertising revenue. In the subscription services model, listeners pay a monthly fee to receive music free from commercial interruptions. Streaming now accounts for two-thirds of the global revenue of the recorded music industry [**108**].

In the video-streaming arena, a variety of subscription services, including Netflix, Amazon Prime Video, Disney+, HBO Max, Paramount+, Apple TV+, and Hulu, provide convenient access to television shows, movies, and original

programming. Over 80 percent of US homes now subscribe to at least one video-streaming service [**109**].

4.7 Protections for Software

In the early days of the computer industry, there was no strong demand for intellectual property protection for software. Most commercial software was produced by the same companies manufacturing computer hardware. They sold complete systems to customers, and the licensing agreements covered use of the software as well as the hardware. Interest in copyrighting software grew with the emergence of an independent software industry in the 1960s.

4.7.1 Software Copyrights

The first software copyrights were applied for in 1964. The Copyright Office allowed the submitted computer programs to be registered, reasoning that a computer program is like a "how-to" book. The Copyright Act of 1976 explicitly recognizes that software can be copyrighted.

When a piece of software gets copyright protection, what exactly is copyrighted? First, copyright protects the original expression of an idea, not the idea itself. For example,

suppose you develop a program for a relational database management system. You may be able to copyright your implementation of a relational database management system, but you cannot copyright the concept of using relational databases to store information.

Second, copyright usually protects the executable program, not the source program. Typically, the source code to a program is confidential, in other words, a trade secret of the enterprise that developed it. The company only distributes the executable program to its customers. The copyright also protects the screen displays produced by the program as it executes. This is particularly valuable for the developers of video games.

4.7.2 Violations of Software Copyrights

The holder of a copyright has a right to control the reproduction of the copyrighted material. The definition of what it means to make a copy of a program is broad. Suppose you purchase a program stored on a CD. If you transfer a copy of the program from the CD to a hard disk, you are making a copy of it. If you execute the program, it is copied from the hard disk of the computer into its random-

access memory (RAM). This, too, is considered making a copy of the program. The standard licensing agreement that comes with a piece of commercial software allows the purchaser of the product to do both of the above-mentioned copying operations.

However, doing any of the following actions without the authorization of the copyright holder is a violation of copyright law:

1. Copying a program onto a CD to give or sell to someone else
2. Preloading a program onto the hard disk of a computer being sold
3. Distributing a program over the Internet

Another kind of copyright violation can occur when a company attempts to create software that competes with an existing product. Two court cases illustrate a copyright infringement and fair use of another company's product.

Apple Computer v. Franklin Computer

In the early 1980s, Franklin Computer Corp. manufactured the Franklin ACE to compete with the Apple II. The Franklin

ACE was Apple II compatible, meaning that programs sold for the Apple II would run on the Franklin ACE without modification. In order to ensure compatibility, the Franklin ACE contained operating-systems functions directly copied from a ROM on the Apple II. Apple Computer sued Franklin for infringing on its copyright. The US Court of Appeals for the Third Circuit ruled in favor of Apple Computer, establishing that object programs are copyrightable.

Sega v. Accolade

Video game maker Accolade wanted to port some of its games to the Sega Genesis console. Sega did not make available a technical specification for the Genesis console, so Accolade disassembled the object code of a Sega game in order to determine how to interface a video game with the game console. Sega sued Accolade for infringing on its copyright. In 1992 the US Court of Appeals for the Ninth Circuit ruled in favor of Accolade, judging that Accolade's actions constituted fair use of the software. It noted that Accolade had no other way of discerning the hardware interface and that the public would benefit from additional video games being available on the Genesis console.

4.7.3 Safe Software Development

An organization must be careful not to violate the copyrights held by its competitors. Even unconscious copying can have serious consequences. Years after hearing the song “He’s So Fine,” George Harrison wrote “My Sweet Lord.” The owner of “He’s So Fine” sued Harrison for copyright infringement and prevailed after a lengthy legal battle. Unconscious copying is a real concern in the software industry because programmers frequently move from one firm to another.

Suppose a company needs to develop a software product that duplicates the functionality of a competitor’s product without violating the competitor’s copyright. For example, in the 1980s companies developing IBM-compatible computers needed to develop their own implementations of the BIOS (basic input/output system). A “clean-room” software development strategy helps ensure a company’s software program does not duplicate any code in another company’s product.

In this strategy two independent teams work on the project. The first team is responsible for determining how the

competitor's program works. It may access the program's source code, if it is available. If it cannot get access to the source, it may disassemble the object code of the competitor's product. It also reads the product's user manuals and technical documentation. The first team produces a technical specification for the software product. The specification simply states how the product is supposed to function. It says nothing about how to implement the functionality.

The second team is isolated from the first team. Members of this team have never seen any code or documentation from the competitor's product. They rely solely on the technical specification to develop, code, and debug the software meeting the specification. By isolating the code developers from the competitor's product, the company developing the competing product can demonstrate that its employees have not copied code, even unconsciously.

Oracle v. Google

Sun Microsystems developed the Java programming language in the 1990s. Java has become one of the world's most popular programming languages, in part because of its interoperability; Java programs are compiled into bytecode that can be executed on any Java virtual machine regardless of the underlying computer hardware. Software engineers at

Sun developed functions for input and output, graphical user interfaces, mathematical calculations, and much more, which were grouped into packages. They also created the Java application programming interface (API), which has declaring code that specifies exactly how programmers should invoke the functions in the various packages.

Sun derived income from Java by licensing it to mobile phone manufacturers, such as Nokia, Motorola, and Research in Motion. In 2005 Google purchased Android, which was developing the Android operating system for mobile phones. Google negotiated with Sun to license the Java libraries, but no deal was reached. At that point, Google's programmers developed a clean-room implementation of Java, but they copied 11,500 lines of declaring code from 37 Java API packages in order to save time. Google released a beta version of Android in 2007.

When Oracle America purchased Sun Microsystems in 2010, it acquired Java. Later that year, Oracle sued Google for copyright infringement. In 2012 the District Court for the Northern District of California ruled that the Java APIs were not copyrightable [**110**]. In 2014 the US Court of Appeals for the Federal Circuit reversed the decision and remanded the case back to the District Court for a second trial, asking the

District Court to determine whether Google's copying of the API declarations was a fair use of copyrighted material [**111**]. At the end of a second District Court trial, a jury ruled in 2016 that Google's use of the function declarations was a fair use of copyrighted material [**112**]. In 2018 the US Court of Appeals for the Federal Circuit ruled that Google's copying of 11,500 lines of declaring code of the 37 Java API packages did not meet any of the four criteria for fair use and violated Oracle's copyright. The Court noted that Google programmers had copied 11,500 lines of declaring code when they were only required to copy 170 lines of code to maintain the same functionality. According to the court, copying 11,330 more lines of code than necessary "weighs against fair use" [**113**].

)

4.7.4 Software Patents

Both copyrights and patents are used to provide intellectual property protection to software. Table 4.3 shows the primary differences between the two.

Table 4.3

	Software Copyright	*Software Patent*
What is protected?	Object program, screen displays	Software process with practical utility
Is getting protection expensive?	No	Yes
Is getting protection time consuming?	No	Yes
Is reverse engineering allowed?	Yes	No

The key differences between the copyright and patent software-protection systems.

Origins of Software Patents

Until the early 1980s, the US Patent and Trademark Office refused to grant patents for computer software. Its position was that a computer program is a mathematical algorithm, not a process or a machine.

However, a US Supreme Court decision in 1981 forced the Patent and Trademark Office to begin considering software patents. In the case of *Diamond v. Diehr*, the Supreme Court ruled that an invention related to curing rubber could be patented. Even though the company's principal innovation was the use of a computer to control the heating of the rubber, the invention was a new process for rubber molding, and hence patentable.

Further court rulings compelled the Patent and Trademark Office to begin issuing patents for a much broader range of software. In 1992 the Court of Appeals for the Federal Circuit considered a patent application from a company that had developed a computerized monitoring device that analyzed signals from an electrocardiograph to determine whether a heart-attack victim was at risk of a dangerous arrhythmia. The court ruled that the software was patentable

because the numbers being manipulated by the computer program represented concrete values in the real world. Further court rulings reinforced the idea that computer software and data structures could be patented in the United States [**114**].

Since then, hundreds of thousands of software patents have been granted [**115**]. Microsoft alone files about 3,000 patent applications every year [**116**]. Companies generate revenue by licensing their software patents to other companies. It's also common for several technology companies to hold patents that cover different but essential components of a commercial product. By signing an agreement to cross-license each other's patents, all the companies are free to bring their own versions of the product to market.

Patent-Holding Companies

Given the value of software patents, it's not surprising that a secondary market for them has arisen. When a company holding patents goes bankrupt, it is typical for its patents to be sold to another company [**117**]. Some companies specialize in holding patents and licensing the rights to use these patents. Patent-holding companies aggressively use the courts to enforce their patent rights; these companies are sometimes referred to by their detractors as **patent trolls**.

Because defending against a patent-infringement lawsuit can easily exceed a million dollars, companies that get sued have a strong motivation simply to settle out of court, putting patent trolls "in a position to negotiate licensing fees that are grossly out of alignment with their contribution to the alleged infringer's product or services" [**118**].

In 1992 inventor Thomas Campana and lawyer Donald Stout formed New Technologies Products (NTP), a patent-holding company. The purpose of the company was never to make anything but was to protect valuable intellectual property. About half of the company's 50 patents were originally held by Telefind Corporation, which went out of business. In 2000 NTP sent letters to several companies, warning them that they were infringing on NTP wireless email patents and inviting them to negotiate licensing rights. One of these letters went to Research In Motion (RIM), maker of the BlackBerry, but RIM did not respond. The next year NTP sued RIM for patent infringement. Instead of settling out of court for a few million dollars, RIM took the case to trial and lost. After more unsuccessful legal maneuvering, RIM in 2006 agreed to pay NTP $612.5 million to settle the patent infringement dispute [**119, 120**].

Harms From Too Many Software Patents

Critics of software patents argue that too many software patents have been granted. A problem faced by patent examiners in the Patent and Trademark Office is knowing what the existing technical knowledge (prior art) in computer programming is. Patent examiners typically look at patents already issued to determine prior art. This works fine for other kinds of inventions, but it doesn't work well for software patents because a significant amount of software was written before software patents were first granted. The consequence is that patent examiners have issued many "bad patents"—patents that would not have been issued if the examiner knew about all the prior art. The Patent Office has also been criticized for granting patents for trivial inventions that would be obvious to any skilled computer programmer.

As a consequence of the sheer volume of software patents, the large number of bad patents, and the number of obvious software inventions that are patented, any company releasing a new product that includes software runs a significant risk of being sued for infringing a software patent owned by someone else. Thousands of patent lawsuits are filed in the United States every year [**121**]. Large corporations are resorting to building stockpiles of their own patents, so that if they are sued for infringing another company's patent, they can retaliate with their own patent-infringement countersuit.

The use of software patents as legal weapons is a perversion of their original purpose [**122**].

Smartphone Patent Wars

In 2009 Nokia filed a lawsuit against Apple, alleging that Apple had violated 10 patents owned by Nokia related to wireless communication, and demanding royalty payments [**123**]. Apple responded by suing Nokia for violating 13 patents owned by Apple [**124**].

Apple also took action against several makers of Android smartphones [**121**]. Of these lawsuits, the dispute between Apple and Samsung is particularly notable. Apple filed a lawsuit in 2011 accusing Samsung of both patent and trademark infringement, claiming Samsung's Galaxy phones and tablets copied the "look and feel" of Apple iPhones and iPads, including rounded corners, tapered edges, use of a home button, slide-to-unlock, and the bounce-back visual effect when a user overscrolls [**125**]. Samsung countersued, claiming Apple had violated Samsung patents on mobile communication technologies. The two corporations filed more suits and countersuits around the globe; by the middle of 2012 the companies were involved in more than 50 lawsuits worldwide [**126**]. Their legal fees exceeded $1 billion [**127**]. Some of the lawsuits were won by Apple, Samsung

prevailed in other cases, and some of the cases were dismissed. Even before the lawsuits were resolved, Android makers began changing portions of their user interfaces to avoid infringing on Apple's patents [**128**].

Eventually, Sony, Google, Samsung, Microsoft, Motorola, Xiamoni, and HTC were drawn into the fray, which acquired the nickname "the smartphone patent wars." More than 100 lawsuits and countersuits were filed by smartphone manufacturers claiming patent violations by their competitors. At the end of 2014, the smartphone makers agreed to cross-license each other's patents [**129**].

Notwithstanding the cross-licensing agreement, legal proceedings continued for years over how much Samsung should have to pay Apple, after a 2012 jury verdict determined that Samsung had infringed on three design patents and two utility patents owned by Apple. That jury had called for Samsung to pay Apple $1 billion in damages. At the end of 2015, Samsung agreed to pay Apple $548 million on the condition that Samsung would be reimbursed if its legal appeal resulted in a smaller judgment [**130**]. In 2018 another trial ended in San Jose, California, with the jury deciding that Samsung should pay Apple $539 million in damages [**131**].

Alice Corporation v. CLS Bank

According to some critics, the smartphone patent wars were a good example of how overly broad software patents were hampering innovation. Many hoped the US Supreme Court would take action to circumscribe patent protection for software. The Supreme Court did just that in 2014 with its decision in *Alice Corporation v. CLS Bank*.

Alice Corporation had been granted several software patents related to managing financial transactions using a third party and an escrow account to ensure that both parties to every transaction meet their obligations. After CLS Bank implemented a computerized financial transaction system, Alice Corporation sued CLS Bank for infringing on its patents. In a unanimous decision, the US Supreme Court ruled against Alice Corporation. It noted that escrow is an abstract idea and managing escrow is a common business method. According to the Court, in order for an abstract idea to be patentable, there must be an "inventive concept"; simply implementing an abstract idea on a computer is not sufficient. The patent claims held by Alice Corporation did not meet that standard and were therefore ineligible for patent protection [**132, 133**].

In the years since the Supreme Court ruling, many district courts and federal courts have cited *Alice Corporation v. CLS Bank* to invalidate hundreds of software patents [**134**]. In one noteworthy case from 2015, a US District judge for the Eastern District of Texas granted the motions of defendants and in a summary judgment threw out 168 patent-infringement lawsuits that had been filed by eDekka (a notorious patent-holding company), ruling that the software patent used as the basis of the lawsuits—"Random Access Information Retrieval Utilizing User-Defined Labels"—was invalid [**135, 136**].

The *Alice* decision has also had a significant impact on the US Patent and Trademark Office (USPTO). After the *Alice* decision the USPTO released new guidelines to patent examiners, and the rejection rate for software patent applications rose sharply [**137, 138**].

In another decision, *Williamson v. Citrix Online*, the US Court of Appeals for the Federal Circuit ruled that a patent for a distributed learning system was invalid because it failed to disclose the structure of the invention [**139**]. The *Williamson* decision sets a precedent for other courts to strike down software patents that are determined to be "too broad and indefinite" [**140**].

4.8 Legitimacy of Intellectual Property Protection For Software

Licenses for proprietary software usually forbid you from making copies of the software to give or sell to someone else. If you violate the license, you are breaching a contract. In this section we are *not* discussing the morality of breaching a contract. Rather, we are considering whether as a society we ought to give the producers of software the right to prevent others from copying the software they produce. In other words, should we give copyright and/or patent protection to software?

Rights- based and consequentialist arguments have been given for granting intellectual property protection to those who create software. Let's review and test the strength of these arguments. To simplify the discussion, we'll assume that a piece of software is written by a person. In reality,

most software is created by teams, and the company employing the team owns the rights to the software the team produces. However, the logic is the same whether the software creator is an individual or a corporation.

4.8.1 Rights-Based Analysis

Not everyone can write good computer programs, and programming is hard work. Programmers who write useful programs that are widely used by others should be rewarded for their labor. That means they should own the programs they write. Ownership implies control. If somebody creates a piece of software, they have the right to decide who gets to use it. Software owners ought to be able to charge others for using their programs. Everybody ought to respect these intellectual property rights.

This line of reasoning is a variation of Locke's natural-rights argument that we discussed at the beginning of the chapter. It is based on the Lockean notion that mixing your labor with something gives you an ownership right in it.

Here are two criticisms of the "just deserts"[1] argument. First, why does mixing your labor with something mean that you own it? Doesn't it make just as much sense to believe that if

you mix your labor with something you lose your labor? Robert Nozick gives this example: If you own a can of tomato juice and pour it in the ocean, mixing the tomato juice with the salt water, you do not own the ocean. Instead, you have lost your can of tomato juice. Certainly, it would be unjust if someone else could claim ownership of something you labored to produce, but if there were no notion of property ownership and everybody understood when they mixed their labor with something they lost their labor, it would be just.

Of course, we do live in a society that has the notion of ownership of tangible property. How can we justify giving a farmer the right to the crop they labor to produce while failing to give a programmer the right to the accounting program they produce for the benefit of the farmer?

Still, if we do want to give ownership rights to those who produce intellectual property, we run into the problem we discussed at the beginning of the chapter. Locke's natural-rights argument for owning property does not hold up well when extended to the realm of intellectual property. There are two crucial differences between intellectual property and tangible property. Each piece of intellectual property must be

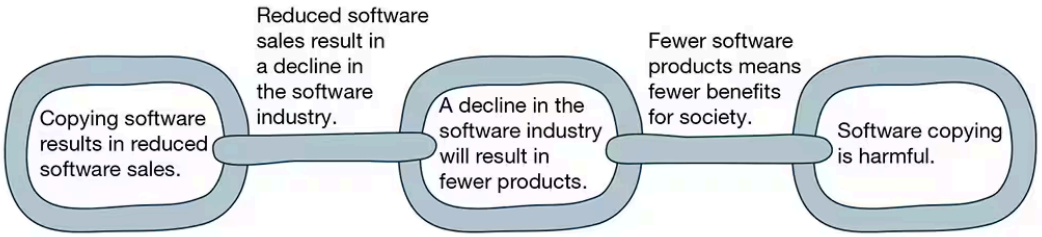
unique in order to be protectable, and copying intellectual property is different from stealing something physical.

4.8.2 Utilitarian Analysis

Another argument posits that failing to provide intellectual property protection for software producers would have harmful consequences overall. The argument goes like this [**141**]: When software is copied, it reduces software purchases. If less software is purchased, less money flows to the producers of software. As a result, less new software is produced. As a whole, new software titles benefit society. When the number of new titles drops, society is harmed. Therefore, when software is copied, society is harmed, and copying software is harmful.

You can view this argument as a chain of consequences (Figure 4.8). Copying software causes software sales to drop, which causes the software industry to decline and, subsequently, fewer products to be released, which causes society to be harmed. Logically, all the links in the chain must be strong in order for the argument to be convincing. Let's look at each of the links in turn.

Figure 4.8


Copying software results in reduced software sales.
Reduced software sales result in a decline in the software industry.
A decline in the software industry will result in fewer products.
Fewer software products means fewer benefits for society.
Software copying is harmful.

The chain of reasoning of a consequentialist argument for why copying software is bad.

(Beth Anderson)

The first claim is that copying software results in reduced sales of software. When talking about software piracy, the computer industry cites the dollar value of the copied software as if each instance of copying represents a lost sale. Obviously, this is an exaggeration. Not everyone who gets a free copy of a computer game has the money or the desire to purchase the game. In fact, sometimes software copying may lead to a sale. A person may not have been interested in buying a particular program. After trying it out for free, the person may decide it is so useful they are willing to buy a copy of the program in order to get access to all the documentation, the technical support line, or another service provided to registered users of the program. It is fair to say that copying software sometimes results in reduced sales of software, but it is not always the case. Hence it is incorrect to make a universal statement.

The second claim is that reduced sales of software result in a decline in the software industry. An argument against this claim is the continued success of Microsoft, despite the fact

that software counterfeiting is prevalent in some countries. A better argument against the claim is that it makes a strong cause-and-effect connection between the creation of software and financial remuneration. However, the open-source movement demonstrates many people are willing to create software without being rewarded financially. Some people write programs because they find it fun. Others are motivated by the desire to gain a good reputation by writing a program many people find useful. Advocates of open-source software, including Richard Stallman, suggest that the best way to stimulate innovation is to allow a free exchange of ideas and source code. From this point of view, allowing software producers to control the distribution of their code stifles, rather than promotes, innovation in the software industry.

Furthermore, the second claim assumes that software customers are solely responsible for the health of the software industry. In reality, other groups want to ensure that there are plenty of new software titles released. Intel, for example, makes its money from selling CPU chips. Every year the chips are faster. If a person owns a computer fast enough to run his current programs, they have little motivation to upgrade the hardware. However, if that same person purchases a new program that requires additional CPU cycles, they may be motivated to upgrade their computer. Hence it is in Intel's

interest to encourage the development of ever more computationally intensive computer programs. Software customers are not solely responsible for promoting the growth of the software industry.

The third claim is that new software packages benefit society. This is a difficult claim to prove. Certainly, some programs benefit society more than others. Hence it's not the number of different programs that matters; it's what they can be used for. The utility of new software titles must be weighed against the utility of letting people give away copies of programs that would help their friends.

;

4.8.3 Conclusion

We have examined two arguments for why society ought to provide intellectual property protection to software creators. The first argument is based on the notion of just deserts. It is a variation of the natural-rights argument we discussed at the beginning of the chapter. This argument is weak; it rests on the faulty assumption that a natural right to own property extends cleanly to intellectual property.

The second argument is based on consequences. It holds that denying intellectual property protection for software would have harmful consequences. It relies upon a chain of cause-

and-effect relationships: copying leads to a loss of revenue, which leads to a decline in software production, which harms society. The strength of each of the links in the chain is debatable; taken as a whole, the argument is not strong.

Our conclusion is that the arguments for granting intellectual property protection for software are not strong. Nevertheless, our society *has granted* copyright protection to owners of computer programs. If you violate a licensing agreement by copying a CD containing a computer program and giving it to a friend, you are breaching a contract. From the viewpoint of Kantianism, rule utilitarianism, and social contract theory, breaching a contract is wrong unless there is a strong overriding moral obligation to do so.

onounced with the accent on the second syllable. Think of the related word leserve."

4.9 Open-Source Software

4.9.1 Evolution of Proprietary Software

In the early years of commercial computing, there was no independent software industry. Computer manufacturers such as IBM produced both the hardware and the software needed for the system to be usable. Well into the 1960s, software distributions included the source code. Customers who wanted to fix bugs in the programs or add new features could do so by modifying the source code and generating a new executable version of the program.

In the 1970s the number of computer applications expanded, and organizations recognized the increasing value of software. To protect their investments in software development, most companies decided to make their programs proprietary.

Today, companies developing proprietary software tightly control the distribution of their intellectual property. Typically, they do this by treating source code as a trade secret and distributing only the object code, which is not in human-readable form. In addition, they do not sell the object code. Instead, when people "purchase" the program, what they are actually buying is a license allowing them to run the program. Their rights to do other things with the code, such as make backup copies, are limited.

Software licensing models have evolved. Until the early 2000s, proprietary license models were the norm. In a proprietary license model, the customer purchases a one-time license to use the software. The customer can use the software in perpetuity, but the customer does not have the right to receive updates or technical support without additional licenses. Subscription models emerged in the early 2000s and have become increasingly popular among software companies. In a subscription model, customers pay a monthly or annual fee to use the software and to receive software updates and technical support [**142**].

Companies developing new software platforms have the option of making their platforms "open" or "closed." An **open platform** has publicly available design and

implementation details, usually based on open standards, that allow independent developers to create new products for the platform. When multiple companies create products based on the same open standards, consumers benefit in several ways. A larger community of developers can enhance innovation and bring new products to market sooner. Competition keeps prices lower. Products from different companies can be combined. Consumers do not have to worry about getting "locked in" to a particular company's product. Google's Android operating system is an example of an open platform.

In a **closed platform** (or **proprietary platform** or **walled garden**), the company keeps tight control over the applications available to users. Closed platforms have some benefits for consumers. By vetting applications, the company can ensure a consistent user experience as well as maintain security and reliability standards. Closed platforms also provide companies the ability to generate revenue from the sale of applications. Apple's iOS operating system is an example of a closed platform.

4.9.2 Consequences of Proprietary Software

Governments have given ownership rights to those who produce computer software because of the perceived beneficial consequences. A key benefit is the ability to profit from the licensing of the software. The assumption is that people will work harder and be more creative if they must compete with others to produce the best product. Those who produce the best products will have the opportunity to make money from them.

While most people point to the benefits of a system encouraging the development of proprietary software, some people have noted the harms caused by such a system. As noted above, a well-known critic of proprietary software is Richard Stallman. According to Stallman, granting intellectual property rights to creators of computer software has numerous harmful consequences [**143**]:

- Digital technology has made copying trivial. In order to enforce copyrights in the digital age, increasingly harsh measures are being taken. These measures infringe on our liberties.
- The purpose of the copyright system is to promote progress, not to make authors wealthy. Copyrights are not promoting progress in the computer software field.

- It is wrong to allow someone to "own" a piece of intellectual property. Granting someone this ownership forces the users of a piece of intellectual property to choose between respecting ownership rights and helping their friends. When this happens, the correct action is clear. If a friend asks you for a copy of a proprietary program, you would be wrong to refuse your friend. "Cooperation is more important than copyright."

The **open-source movement** is the philosophical position that source code to software ought to be freely distributed and that people should be encouraged to examine and improve each other's code. The open-source software movement promotes a cooperative model of software development.

}

4.9.3 "Open Source" Definition

Open source is an alternative way of distributing software. Numerous definitions of open source exist. According to the Open Source Initiative, licenses for open-source programs have the following key characteristics (there are others) [144]:

1. There are no restrictions preventing others from selling or giving away the software.
2. The source code to the program must be included in the distribution or easily available by other means (such as downloadable from the Internet).
3. There are no restrictions preventing people from modifying the source code, and derived works can be distributed according to the same license terms as the original program.
4. There are no restrictions regarding how people can use the software.
5. These rights apply to everyone receiving redistributions of the software without the need for additional licensing agreements.
6. The license cannot put restrictions on other software that is part of the same distribution. For example, a program's open-source license cannot require all the other programs on the CD to be open source.

Note that there is nothing in these guidelines that says an open-source program must be given away for free. While people may freely exchange open-source programs, a

company has the right to sell an open-source program. However, a company cannot stop others from selling it either. In order for a company to be successful selling open-source software that people can find for free on the Internet, it must add some value to the software. Perhaps it packages the software so that it is particularly easy to install. It may provide great manuals, or it may provide support after the sale.

The Open Source Initiative (**www.opensource.org**) is a nonprofit corporation that promotes a common definition of open source. In July 2023, its Web site listed the names of more than 90 software licenses that met its definition of open source.

4.9.4 Beneficial Consequences of Open-Source Software

Advocates of open-source software describe five beneficial consequences of open-source licensing.

The first benefit of open source is that it gives everyone using a program the opportunity to improve it. People can fix bugs,

add enhancements, or adapt the program for entirely new uses. Software evolves more quickly when more people are working on it.

Rapid evolution of open-source software leads to the second benefit: new versions of open-source programs appear much more frequently than new versions of commercial programs. Users of open-source programs do not have to wait as long for bug fixes and patches [**145**].

A third benefit of open source is that it eliminates the tension between obeying copyright law and helping others. Suppose you legally purchased a traditional license to use a program and your friend asks you for a copy. You must choose between helping your friend and conforming to the license agreement. If the program had an open-source license, you would be free to distribute copies of it to anyone who wanted it.

The fourth benefit is that open-source programs are the property of the entire user community, not just a single vendor. If a vendor selling a proprietary program decides not to invest in further improvements to it, the user community is stuck. In contrast, a user community with access to the

source code of a program may continue its development indefinitely [**145**].

The fifth benefit of open source is that it shifts the focus from manufacturing to service, which can result in customers getting better support for their software [**145**]. If source code were distributed freely, companies would make money by providing support, and the companies that provided the best support would be rewarded in the marketplace [**146**].

4.9.5 Examples of Open-Source Software

Open- source software is a key part of the Internet's infrastructure, and an increasing number of open-source applications are reaching the desktop. Here are a few examples of highly successful programs distributed under open-source licenses:

- BIND provides DNS (domain name service) for the entire Internet.
- Apache runs about one-third of the world's Web servers.

- The most widely used program for moving email about the Internet is the open-source program sendmail.
- The Android operating system is the world's best-selling smartphone platform [**147**].
- Firefox is the world's number-four Web browser [**148**].
- OpenOffice.org is an office application suite supporting word processing, spreadsheets, databases, and presentations.
- Perl is the most popular Web programming language.
- Other popular open-source programming languages and tools are Python, Ruby, TCL/TK, PHP, and Zope.
- Programmers have long recognized the high quality of the GNU compilers for C, C++, Objective-C, Fortran, Java, and Ada.

Surveys indicate that the quality and dependability of open-source software is about the same as that of commercial software [**149**].

4.9.6 The GNU Project and Linux

The GNU Project and Linux are important success stories in the history of the open-source movement. (GNU is pronounced “guh-new” with the accent on the second syllable. It’s a tradition among hackers to invent recursive acronyms; GNU stands for “GNU’s Not Unix.”) Richard Stallman began the GNU Project in 1984. The goal of the project was ambitious: to develop a complete Unix-like operating system consisting entirely of open-source software.

)

In order to be fully functional, a modern operating system must include text editors, command processors, assemblers, compilers, debuggers, device drivers, mail servers, and many other programs. During the late 1980s, Stallman and others developed most of the necessary components. The GNU Project also benefited from open-source software previously developed by others, notably Donald Knuth’s T_EX typesetting system (used to typeset this book) and MIT’s X Window System. Most of the software developed as part of the GNU Project is distributed under the GNU Public License, an example of an open-source license. (For technical reasons some programs have been distributed as open-source software under other licenses.)

In 1991 Linus Torvalds began work on a Unix-like kernel he named Linux. (The kernel is the software at the very heart of

an operating system.) He released version 1.0 of the kernel in 1994. Because the other major components of a Unix-like operating system had already been created through the GNU Project, Torvalds was able to combine all the software into a complete, open-source, Unix-like operating system. To the obvious chagrin of Stallman, Linux has become the commonly accepted name for the open-source operating system based on the Linux kernel. (Stallman urges people to refer to the entire system as GNU/Linux [**150**].)

4.9.7 Impact of Open-Source Software

In 1998 Andrew Leonard summarized the impact of Linux this way: "Linux is subversive. Who could have thought even five years ago that a world-class operating system could coalesce as if by magic out of part-time hacking by several thousand developers scattered all over the planet, connected only by the tenuous strands of the Internet?" [**146**].

Linux has become a viable alternative to proprietary versions of Unix. Many companies adopted Linux as a way to cut costs during the recession of 2008–2009 [**151**]. A survey conducted in June 2022 revealed that 48 percent of the

world's 500 fastest supercomputers were running the Linux operating system [**152**].

4.10 Creative Commons

As we saw earlier in this chapter, some believe strong intellectual property protection stimulates creativity by dangling the prospect of financial reward in front of artists and inventors. Others believe that creativity is suppressed in such an environment. They argue that people are more creative when they are free to build on the work of others. Consider music, for example. It's not just rap musicians who sample the works of others to create new songs. Listen to the classical piece Appalachian Spring by Aaron Copland and you'll find that he used the Shaker hymn "Simple Gifts."

Information technology has created an environment in which an unprecedented amount of creativity could be unleashed. Never before has it been so inexpensive to record and mix music, combine photographs and computer-generated images, or tape and edit movies. Wouldn't it be great to take what others have done and add your own talents to produce even better works of art for everyone's enjoyment? Quoting the movie *Get Creative* on the Creative Commons Web site: "Collaboration across space and time. Creative co-authorship

with people you've never met. Standing on the shoulders of your peers. It's what the Internet is all about" [153].

Strong intellectual property protection, however, stands in the way of this vision. Under current US copyright law, works of intellectual property are copyrighted the moment they are made, even if the creator does not attach a copyright symbol © to the work. Since copyright is implicit, permission is required before use. The current system discourages people from building on the work of others.

Imagine the difficulty an art professor has trying to put together a Web site of images for an online course! They need to request permission for every image they wish to display on the Web site. Suppose there are three suitable images of Michelangelo's *Pietà*. It may be impossible for them to tell in advance which, if any, of the photographers would be willing to let them use the image. It would be better if there were an official way for a photographer to say, "It's fine if you use this photograph, as long as you give me credit for taking it."

Stanford law professor Lawrence Lessig realized there was a need for a system that would allow producers of intellectual property to indicate to the world the rights they wanted to keep. Lessig asks us to think about instances of the **commons**, a "resource to which anyone within the relevant community

has a right without obtaining the permission of anyone else" [**154**, pp. 19–20]. Examples of the commons include public streets, parks, beaches, the theory of relativity, and the works of Shakespeare. Lessig says that "there is a benefit to resources held in common and the Internet is the best evidence of that benefit. . . . The Internet forms an *innovation commons*" [**154**, p. 23]. The reason Lessig calls the Internet an innovation commons is because its control is decentralized: one person can introduce a new application or new content without getting anyone else's permission.

Lessig joined with Hal Abelson, James Boyle, Eric Eldred, and Eric Saltzman to found the nonprofit corporation Creative Commons in 2001. Creative Commons provides standard copyright licenses free of charge. Every license comes in three forms: human-readable, lawyer-readable, and computer-readable. With a Creative Commons license, you can retain the copyright while allowing some uses of your intellectual property under certain circumstances. Because you have published the circumstances under which your work may be used, others do not have to ask for permission before using your work [**153**].

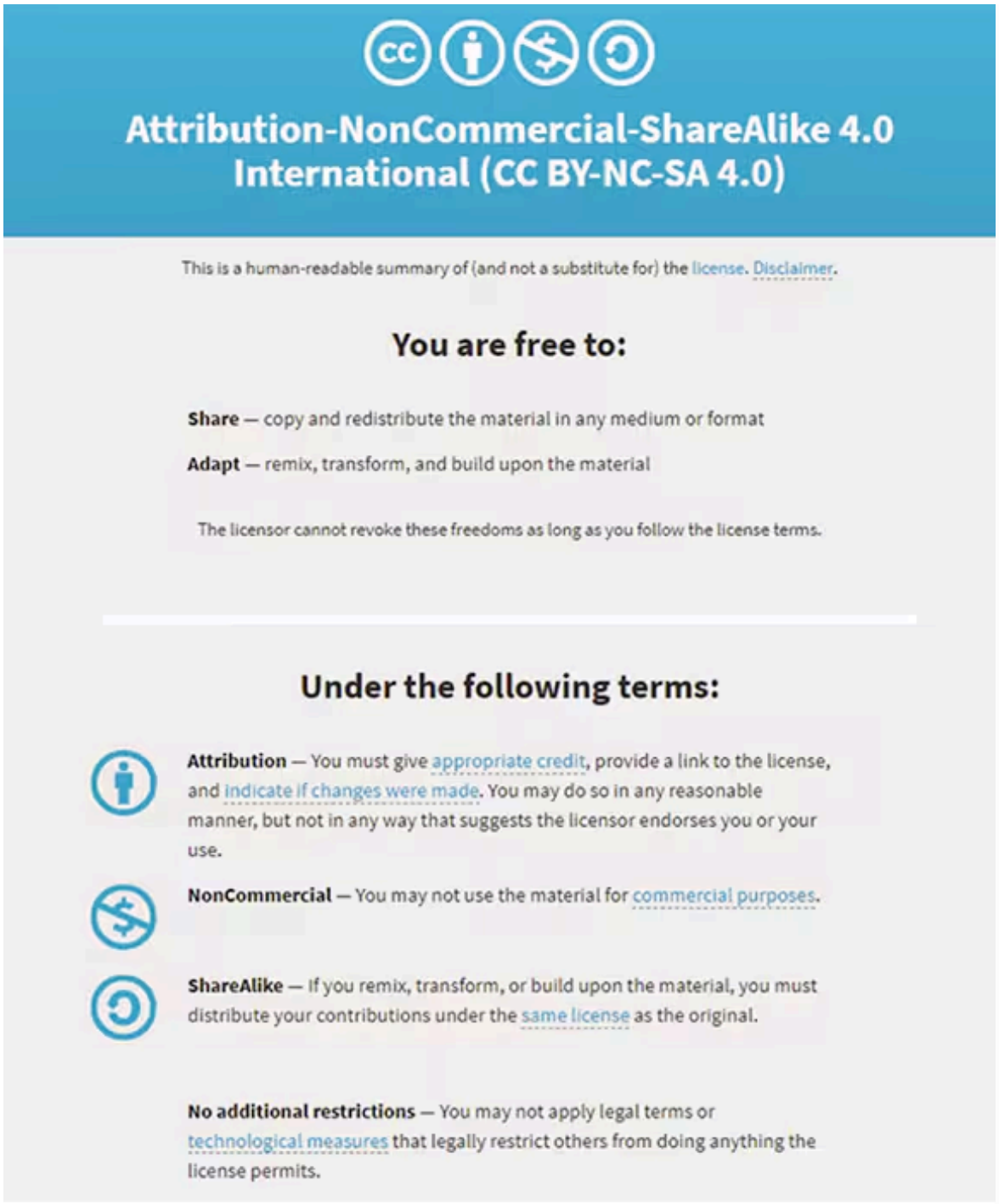
How does the system work? Suppose you have taken a photograph and wish to post it on your Web site

accompanied by a Creative Commons license. You visit the Creative Commons Web site (www.creativecommons.org), which allows you to choose between six different licenses, depending upon your responses to two questions (quoted verbatim):

- Allow adaptations of your work to be shared?
  - Yes
  - No
  - Yes, as long as others share alike
- Allow commercial uses of your work?
  - Yes
  - No

After you answer these two questions, the Web site creates HTML code containing the appropriate Creative Commons license. You can copy the HTML code and paste it into the appropriate Web page along with your photograph. Visitors to your Web site will be able to see a human-readable summary of the license you have chosen (Figure 4.9).

Figure 4.9


Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)
This is a human-readable summary of (and not a substitute for) the license. Disclaimer.
You are free to:
Share — copy and redistribute the material in any medium or format
Adapt — remix, transform, and build upon the material
The licensor cannot revoke these freedoms as long as you follow the license terms.
Under the following terms:
Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
NonCommercial — You may not use the material for commercial purposes.
ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.
No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

A portion of the human-readable summary of a Creative Commons license as it appears to a Web site visitor.

(Screenshot from Creative Commons. Copyright © 2018 by Creative

Commercial artists may choose to use Creative Commons licenses to increase exposure to their work. For example, suppose you take a great photograph of the Golden Gate Bridge. You post it on your Web site with a Creative

Commons license indicating the photograph may be used for noncommercial purposes as long as the user gives attribution to you. People from around the world think the image is stunning, and they copy it to their own personal Web sites, giving you credit for the photo. A travel agent in a foreign country sees the image and wants to put it on a travel poster. Since this is a commercial purpose, they must gain your permission before using the image. At that time you can negotiate a fair price for its use. Without the widespread distribution of the image through a Creative Commons license, the travel agent might never have seen it.

The computer-readable versions of the licenses are designed to make it easier for search engines to identify content based upon the particular criteria. For example, a history professor might use a search engine hoping to find an image of the Coliseum in Rome that they could include on their Web site. Their purpose is noncommercial and they are happy to credit the photographer, but they do not want to have to pay to display the image or write a letter asking for the photographer's permission. A search engine could return only those images that meet these criteria.

By 2008, about 130 million different pieces of intellectual property had been distributed using Creative Commons

licenses. In 2009 the Creative Commons Attribution-ShareAlike license became the principal content license for *Wikipedia*. In 2023 Flickr alone had more than 475 million photos available under Creative Commons licenses [**155**].

Summary

At the beginning of Chapter 2 we noted how forming communities allows us to enjoy better lives than if we lived in isolation. One of the advantages of community life is being able to enjoy the fruits of other people's creativity, and we do in fact spend much of our time enjoying entertainment created by others—television shows, movies, music, and games—delivered on electronic devices that are also the fruits of human ingenuity. It should come as no surprise, then, that our society promotes the creation of intellectual property.

To stimulate creativity in technology and the arts, governments have decided to grant limited ownership rights to the creators of intellectual property, giving them the opportunity for financial gain. In the United States, there are four different ways in which individuals and organizations can protect their intellectual property: trade secrets, trademarks/service marks, patents, and copyrights. The purpose of these protections is to provide creators of intellectual property with a proper financial reward for their efforts, while ensuring the public has access to their creations.

The fair-use doctrine is an example of a government trying to strike the proper balance between the rights of the intellectual property creator and the common good. Time-shifting television programs, space-shifting music, and the Google Books project are three important examples of fair use of copyrighted material.

The introduction of digital technology and the Internet have brought intellectual property issues to the forefront. Representing audio and video content digitally means anyone with the right equipment can make perfect copies. Broadband Internet technology enables these copies to be quickly and widely disseminated. The Pirate Bay is a prime example of an organization leveraging these two technological breakthroughs to make copyrighted material freely available. Producers of copyrighted material have responded by trying to shut down the Pirate Bay and putting new restrictions on copying, even though sometimes these restrictions have made it impossible for consumers to make copies that were previously considered fair use. To a large extent, these efforts have been unsuccessful. Companies trying to sell access to movies, television shows, and songs now understand that they need to make "doing the right thing"—obtaining a legal copy—as easy as "doing the wrong thing." It is now more

convenient to stream paid content than it is to get illegal copies through the Pirate Bay.

Until the mid-1960s, there was no intellectual property protection for computer software other than trade secrets. Now, both copyrights and patents are used to protect software. The area of software patents is highly controversial. There are a large number of bad software patents, and many software patents have been issued for obvious inventions. Large corporations are stockpiling software patents, so that if they are sued for infringing another company's patent, they can retaliate with their own patent-infringement countersuit. The decision of the US Supreme Court in *Alice Corporation v. CLS Bank* may prove to be a turning point. Many district courts and federal courts have cited that decision to invalidate hundreds of software patents.

There are both rights-based and utilitarian arguments as to why we ought to give intellectual property protection to software; neither of these arguments is particularly strong, suggesting that there should be an alternative to a conventional proprietary model of software development. The open-source movement is such an alternative. A great deal of the software that keeps the Internet running is open-source software. Other open-source success stories include

the Linux and Android operating systems, the Firefox browser, and OpenOffice productivity software.

The story of the GNU Project and Linux demonstrates how thousands of volunteers can work together to produce high-quality, industrial-strength software. Why can't the success of GNU/Linux be replicated in the arts? Imagine a culture that encouraged the production of new creative works from existing works, a culture in which songs would rapidly evolve, different versions of movies were exchanged and compared, and hypertext novels accumulated links to fan sites. Today's intellectual property laws make it difficult to achieve this vision in the entertainment field. Little can be done with a copyrighted work without first asking for permission, a labor-intensive process that puts a drag on innovation. Creative Commons is an effort to streamline the process by allowing copyright holders to indicate up front the conditions under which they are willing to let other people use their work.

Further Reading, Listening, and Viewing

Kornhaber Brown. “F.A.T. Lab.” Off Book, September 13, 2011. 8:38. video.pbs.org.

Charles Duhigg and Steve Lohr. “The Patent, Used as a Sword.” *New York Times*, October 7, 2012.

David Friedman. “The First Software Patent.” PBS Digital Studios, January 24, 2013. 4:34. www.youtube.com/watch?v=yKdqJGgpcgg.

C. G. P. Grey. “Copyright: Forever Less One Day.” 6:28. www.youtube.com/watch?v=tk862BbjWx4.

Leah Hoffmann. “Open for Business.” *Communications of the ACM*, Vol. 55, No. 4, April 2012.

Gwen Ifill. “How Effective Is Justice Department Crackdown on Online Sale of Counterfeit Goods?” PBS *NewsHour*, November 29, 2011. 9:13. video.pbs.org.

Steven Levy. “The Patent Problem.” *Wired*, December 4, 2012. www.wired.com.

Ephrat Livni, Lauren Hirsch, and Sarah Kessler. “Who Owns a Song Created by A.I.?” *New York Times*, April 15, 2023. https://www.nytimes.com/2023/04/15/business/dealbook/artific intelligence-copyright.html.

Steve Lohr. “Can A.I. Invent?” *New York Times*, July 15, 2023. https://www.nytimes.com/2023/07/15/technology/ai inventor patents.html.

Peter S. Menell. “Design for Symbiosis.” *Communications of the ACM*, Vol. 55, No. 5, May 2012.

Nilay Patel. “Slide to Unlock: How Apple’s Patents Are Changing Android.” *Verge*, March 6, 2012. theverge.com.

Randal C. Picker. “The Yin and Yang of Copyright and Technology.” *Communications of the ACM*, Vol. 55, No. 1, January 2012.

Robert Shore. “The Art of the Steal: When Does a Copyright Go Too Far?” *New York Times*, November 23, 2017. https://www.cnn.com/style/article/art copyright beg steal borrow/index.html.

Ben Sisario. “Stolen or Original? Hear Songs From 7 Landmark Copyright Cases.” *New York Times,* April 27, 2023. https://www.nytimes.com/2023/04/27/arts/music/music copyright lawsuits ed sheeran blurred lines.html.

Matt Stevens. “After the Warhol Decision, Another Major Copyright Case Looms.” *New York Times*, May 22, 2023. https://www.nytimes.com/2023/05/22/arts/warhol prince decision copyright.html.

Zach Weissmueller. “Too Much Copyright.” ReasonTV (Web site), April 19, 2012. 8:57. www.youtube.com/watch?v=rFMl0stqai0.

“Can Fan Culture Change Society?” *Off Book,* September 7, 2012. 6:49. video.pbs.org.

“Open Source Basics.” Intel Software, June 6, 2014. 5:41. www.youtube.com/watch?v=Tyd0FO0tko8.

“What Is Open Source?” *Mozilla,* April 18, 2017. 2:51. www.youtube.com/watch?v=7c0IrsDsNaw.

Review Questions

1. What features of intellectual property make it more difficult to protect than physical property?
2. What paradoxes arise when we attempt to extend Locke's notion of a natural right to property into the realm of intellectual property?
3. What are the ways in which individuals or firms in the United States may protect their intellectual property?
4. What are the relative advantages and disadvantages of patents versus trade secrets?
5. The case study in Section 4.3.5 evaluates two possible actions by Rajiv. Perform act-utilitarian evaluations of two other actions Rajiv could take:

   Option 3: Rajiv does not ask the team of software developers to improve the design of the database system. He allows the team to proceed with the implementation based on the current design.

Option 4: Rajiv meets the team of software developers implementing the database system, shares with them the optimizations he developed at Felicity Software, and asks the team to incorporate his optimizations into the system.

6. When referring to copyrighted materials, what is meant by the term “fair use”?

7. Explain how advances in information technology have made it easier for consumers to violate copyright law.

8. How has the Digital Millennium Copyright Act affected fair use of copyrighted material by consumers?

9. How does BitTorrent provide an order-of-magnitude increase in downloading speed compared to earlier peer-to-peer networks?

10. The US Supreme Court ruled that Sony was not responsible for the copyright infringements of Betamax customers, but Grokster and StreamCast were responsible for the copyright infringements of those who used their peer-to-peer networks. Explain the differences in the two situations that led the Supreme Court to reach opposite conclusions.

11. Briefly describe the most significant changes in the recorded music business in the United States over the past 15 years.

12. Suppose company A wants to develop a program that duplicates the functionality of a program made by company B. Describe how company A may do this without violating the copyrights held by company B.

13. What are the differences between an open system and a closed system? What are the advantages of each type of system?

14. When describing a software license, what does the phrase “open source” mean?

Discussion Questions

15. Benjamin Franklin created many useful inventions without any desire to receive financial reward. Is intellectual property protection needed in order to promote innovation?

16. Any original piece of intellectual property you have created, such as a poem, term paper, or photograph, is automatically copyrighted, even if you did not label it with a copyright notice. Think about the most valuable piece of intellectual property you have ever created. Describe in detail the ownership rights you would like to claim on it.

17. Do you support the aims of the Google Books project? Does this initiative give Google too much power?

18. How does the debate over digital music illuminate the differences among ethics, morality, and law?

19. Is the concept of digital rights management doomed to failure?

20. What does the US Supreme Court decision in *MGM v. Grokster* mean for the development of future peer-to-peer network technologies?

21. The current legal system allows both proprietary software and open-source software to be distributed. What are the pros and cons of maintaining the status quo?

22. Examine the analyses of Section 4.8 regarding the legitimacy of providing intellectual property protection for software. Do these arguments apply equally well to the question of providing intellectual property protection for music? Why or why not?

23. Should copyright laws protect musical compositions? Should copyright laws protect recordings of musical performances?

24. Is it hopeless to try to protect intellectual property in digital media?

In-Class Exercises

25. A plane makes an emergency crash landing on a deserted tropical island. Two dozen survivors must fend for themselves until help arrives. All of them are from large cities and none of them has camping experience. The survivors find it impossible to gather enough food, and everyone begins losing weight. One person spends a lot of time alone and figures out how to catch fish. They bring fish back to the camp. Others ask them to teach them how to catch fish. They refuse but offer to share the fish they have caught with the other passengers as long as they take care of the other camp chores, such as hauling fresh water, gathering firewood, and cooking.

    Divide the class into groups of about four persons each. Half the groups should come up with reasons why the fisherman's position is morally wrong, and the remaining groups should come up with reasons why the fisherman's position is morally acceptable. After a reasonable amount of time, the teams should take turns sharing their reasons with the rest of the class.

26. Survey 10 of your peers with these questions. How many own CDs? How many own DVDs? How many rely entirely upon streaming for watching videos and listening to music? Share the results with your classmates.

27. Research your university's policy on bandwidth abuse and file sharing. What kinds of activities are explicitly forbidden? Is the policy sensible?

References

[1] Jordan Simon. “Jimmy Fallon and Addison Rae under Fire for Segment on TikTok Dances, Mostly from Black Creators.” *Shadow and Act*, March 30, 2021. https://shadowandact.com/jimmy-fallon-and-addison-rae-under-fire-for- segment-on-tiktok-dances-mostly-from-black-creators.

[2] Marianne Garvey. “Jimmy Fallon Responds to Backlash over Addison Rae TikTok Dance Segment.” *CNN*, April 6, 2021. https://www.cnn.com/2021/04/06/entertainment/jimmy-fallon-addison-raes-tiktok/index.html.

[3] “Cell Phones Taking Center Stage at Concerts.” RedOrbit (Web site), May 16, 2008. www.redorbit.com.

[4] Aditya Ramesh, Prafulla Dhariwal, Alex Nichol, Casey Chu, and Mark Chen. “Hierarchical Text Conditional Image Generation with CLIP Latents.” ArXiv: 2204.06125, April 13, 2022.

[5] Simmone Shaw. “Netflix Is Cracking Down on Password Sharing in the U.S. Here’s What to Know.”

TIME, May 26, 2023. https://time.com/6282750/netflix-password-sharing-household-rules/.

[6] World Intellectual Property Organization. "What Is Intellectual Property?" Accessed September 30, 2017. www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_4

[7] John Locke. *Two Treatises of Government*. Cambridge University Press, Cambridge, England, 1988.

[8] Michael J. Scanlan. "Locke and Intellectual Property Rights." In *Intellectual Property Rights in a Networked World*, edited by Richard A. Spinello and Herman T. Tavani, pp. 83–98. Information Science Publishing, Hershey, PA, 2005.

[9] Edmund S. Morgan. *Benjamin Franklin*. Yale University Press, New Haven, CT, 2002.

[10] Randolph P. Luck. "Letter to The Honorable Senator Spencer Abraham." Luck's Music Library, June 28, 1996.

[11] Justice Breyer, dissenting. Supreme Court of the United States. Eric Eldred, et al. v. John D. Ashcroft, No. 01-618 (January 15, 2003).

[12] Kembrew McLeod. *Freedom of Expression(R): Overzealous Copyright Bozos and Other Enemies of Creativity*. Doubleday, New York, NY, 2005.

[13] Lawrence Lessig. "The Same Old Song." *Wired*, July 2005.

[14] "Happy Birthday, We'll Sue." Snopes.com (Web site). Urban legends reference pages, April 27, 2007. www.snopes.com.

[15] Robert Brauneis. "Copyright and the World's Most Popular Song." GWU Legal Studies Research Paper No. 1111624, George Washington University Law School, Washington, DC, March 21, 2008.

[16] US District Court, Southern District of New York. Good Morning to You Productions Corp., On Behalf of Itself and All Others Similarly Situated, v. Warner/Chappell Music, Inc. (June 13, 2013).

[17] US District Court, Central District of California. Good Morning to You Productions Corp. v. Warner/Chappell Music, Inc. CV 13-04460-GHK (June 30, 2016).

[18] Bernard Weinraub. "Art Buchwald Awarded $150,000 in Suit Over Film." *New York Times,* page C13, Vol. CXLI, No. 48908, March 17, 1992.

[19] US Patent and Trademark Office. “Trademark Basics.” Accessed October 1, 2017. www.uspto.gov/trademarks-getting-started/trademark-basics.

[20] US Patent and Trademark Office. “Trademark Process.” Accessed October 1, 2017. www.uspto.gov/trademarks-getting-started/trademark-process.

[21] “General Trademark Guidelines.” Adobe Systems Inc. Accessed October 5, 2013. www.adobe.com/misc/trade.html.

[22] International Trade Association, US Department of Commerce. “How Do I Obtain a Patent?” July 7, 2016. www.stopfakes.gov/article?id=How-Do-I-Obtain-a-Patent.

[23] “AT&T’s History of Invention and Breakups.” *New York Times,* February 13, 2016. https://www.nytimes.com/interactive/2016/02/12/technology/at history.html.

[24] United States Court of Appeals, Federal Circuit. Polaroid Corporation, Plaintiff-Appellee, v. Eastman Kodak Company, Defendant-Appellant. Appeal No. 86-604. 789 F.2d 1556 (April 25, 1986).

[25] Lawrence Edelman. “Kodak Pays Polaroid $925M; Part of a Surprise Out-of-Court Settlement Ends 15-Year Legal Hassle.” *Boston Globe*, July 16, 1991.

[26] Kim Peterson. “Microsoft Eases Its Rules for Access to Technology.” *Seattle Times*, December 4, 2003.

[27] Agfa Monotype Corp. “Agfa Monotype Licenses ClearType from Microsoft” (press release). December 12, 2003. whattheythink.com/news/20333-agfa-monotype-licenses-cleartype- microsoft/.

[28] International Intellectual Property Alliance. “Copyright Industries in the U.S. Economy: 2022 Report.” Washington, DC, December 2022. www.iipa.org.

[29] United States Court of Appeals for the Second Circuit. Gershwin Publishing Corporation, Plaintiff-Appellee, v. Columbia Artists Management, Inc., Defendant-Appellant, and Community Concerts, Inc., Defendant, 443 F.2d 1159 (May 24, 1971).

[30] “Millbury Man Pleads Guilty in ‘Davey Jones’ Computer Case.” *Worcester Telegram & Gazette*, December 16, 1994.

[31] Siva Vaidhyanathan. *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens*

Creativity. New York University Press, New York, NY, 2001.

[32] Suzanne Fields. "Free Mickey Mouse (and Robert Frost)." *Jewish World Review*, January 24, 2003.

[33] Chris Sprigman. "The Mouse That Ate the Public Domain: Disney, the Copyright Term Extension Act, and Eldred v. Ashcroft." FindLaw Legal News and Commentary, March 5, 2002. writ.news.findlaw.com.

[34] "Brief for Petitioners." Supreme Court of the United States. Eric Eldred et al. v. John D. Ashcroft, in his official capacity as Attorney General. 2002.

[35] "Eldred v. Ashcroft: A Primer." *WashingtonPost.com*, January 15, 2003.

[36] Supreme Court of the United States. Eldred et al. v. Ashcroft, *Attorney General*, 239 F.3d 372, affirmed (January 15, 2003).

[37] "Beeple's NFT Digital Arft Nets £50m at Christie's Auction." *BBC News,* March 11, 2021. https://www.bbc.com/news/technology-56362174.

[38] "What Are NFTs and Why Are Some Worth Millions?" *BBC News,* December 16, 2022.

https://www.bbc.com/news/technology-56371912.

[39] "Employee Confidentiality and Proprietary Rights Agreement (CA)." Practical Law (Web site). Accessed August 7, 2015. practicallaw.com/3-518-4653.

[40] Kathleen Amen, Tish Keogh, and Necia Wolff. "Digital Copyright." *Computers in Libraries*, May 2002.

[41] Elina M. Lae. "Mashups—a Protected Form of Appropriation Art or a Blatant Copyright Infringement?" SSRN (Web site), December 2011. papers.ssrn.com.

[42] Supreme Court of the United States. Sony Corporation of America et al. v. Universal City Studios, Inc., et al., 464 US 417 (January 17, 1984).

[43] United States Court of Appeals for the Ninth Circuit. Leslie A. Kelly v. Arriba Soft Corporation, 336 F.3d 811 (July 7, 2003).

[44] "About Google Books." Accessed August 13, 2009. books.google.com/intl/en/googlebooks/about.html.

[45] US District Court, Southern District of New York. Authors Guild et al. v. Google Inc., 05 CIV 8136 (September 20, 2005).

[46] US District Court, Southern District of New York. McGraw-Hill Companies et al. v. Google Inc., 05 CV 8881 (October 19, 2005).

[47] US District Court, Southern District of New York. Authors Guild, Inc., et al. v. Google Inc., 1:05-cv-08136-DC (November 14, 2013).

[48] Corynne McSherry. "Court Upholds Legality of Google Books: Tremendous Victory for Fair Use and the Public Interest" (press release). Electronic Frontier Foundation, November 14, 2013. www.eff.org.

[49] US Court of Appeals for the Second Circuit. The Authors Guild et al. v. Google, Inc., 13-4829-cv (October 16, 2015).

[50] US Supreme Court. Orders in Pending Cases, Order List: 578 U.S. (April 18, 2016).

[51] Steven Andersen. "How Piracy, Culture and High-Tech Hackers Brought the Recording Industry to Its Knees." *Corporate Legal Times*, November 2002.

[52] David Goldman. "Music's Lost Decade: Sales Cut in Half." *CNNMoney*, February 3, 2010. money.cnn.com.

[53] Christopher May. "Digital Rights Management and the Breakdown of Social Norms." *First Monday,* Vol. 8,

No. 11, November 2003.

[54] Royal Van Horn. "The Digital Millennium Copyright Act and Other Egregious Laws." *Phi Delta Kappan*, November 2002.

[55] Kelly McCollum and Peter Schmidt. "How Forcefully Should Universities Enforce Copyright Law on Audio Files?" *Chronicle of Higher Education*, November 11, 1999.

[56] Ron Harris. "Where's SDMI? Digital Music Protection Effort Flames Out." *Associated Press*, April 29, 2002.

[57] Kevin Coughlin. "Cyber Music Makers Seek to Gag Code-Breakers." *Newhouse News Service*, April 24, 2001.

[58] John Markoff. "Scientists Drop Plan to Present Music-Copying Study That Record Industry Opposed." *New York Times*, April 27, 2001.

[59] "A Speed Bump vs. Music Copying: Master Cryptographer—and Code Cracker—Edward Felten Says Technology Isn't the Answer to Digital Copyright Violations." *Business Week Online*, January 9, 2002.

[60] "FAQ: Sony's 'Rootkit' CDs." CNet News (Web site), November 21, 2005. news.cnet.com.

[61] "Sony BMG Settlement FAQ." Electronic Frontier Foundation. Accessed September 29, 2015. www.eff.org/IP/DRM/Sony-BMG.

[62] Selena Kim. "The Reinforcement of International Copyright for the Digital Age." *Intellectual Property Journal*, Vol. 16, pp. 93–122, 2003.

[63] Tom Espiner. "British Library Calls for Digital Copyright Action." CNet News (Web site), September 25, 2006. news.cnet.com.

[64] Ali Matin. "Digital Rights Management (DRM) in Online Music Stores: DRM-Encumbered Music Downloads' Inevitable Demise as a Result of the Negative Effects of Heavy-Handed Copyright Law." *Entertainment Law Review*, Vol. 28, Loyola Law School, Los Angeles, CA, 2008.

[65] Michael Arrington. "EMI, Apple to Sell DRM-Free Music for $1.29/Song." *Tech-Crunch*, April 2, 2007. techcrunch.com.

[66] Jacqui Cheng. "Amazon Rounds Out DRM-Free Music Offering with Sony BMG." Ars Technica (Web site),

January 10, 2008. arstechnica.com.

[67] "iTunes Store and DRM-Free Music: What You Need to Know." *MacWorld*, January 7, 2009. www.macworld.com.

[68] Marc Whitten. Letter to Xbox Live members, June 10, 2013. news.xbox.com.

[69] Michael Rundle. "Microsoft Unveils Xbox One Privacy and Digital Rights Details Ahead of E3." *Huffington Post UK*, June 7, 2013. www.huffingtonpost.co.uk.

[70] William Usher. "PS4 Grabs 95 Percent of Consumer Votes After Amazon Ends Poll Early." CinemaBlend (Web site), June 16, 2013. www.cinemablend.com.

[71] Don Mattrick. "Your Feedback Matters—Update on Xbox One." *Xbox Wire*, June 19, 2013. news.xbox.com.

[72] Danielle Roy. "Napster Timeline." IDG News Service, Boston Bureau, April 2, 2001.

[73] Nathan Ruegger. "Napster Withers Away, but Peer-to-Peer Legacy Remains." *Dartmouth*, October 3, 2002.

[74] Ron Harris. "Bankruptcy Judge Blocks Sale of Napster to Bertelsmann." Associated Press, September 4, 2002.

[75] Reuters. “Music Industry Sends Warnings to Song Swappers.” *NYTimes.com*, April 29, 2003.

[76] Phil Hardy. “Verizon Agrees to Give the RIAA the Names of Four Subscribers Alleged to Be File-Sharing Copyrighted Works.” *Music & Copyright*, June 11, 2003.

[77] Sara Calabro. “RIAA Lawsuits—Music Industry Mistakes Its Lawsuits for a PR Maneuver.” *PR Week*, September 22, 2003.

[78] Phil Hardy. “Media Reaction to RIAA’s New Round of Lawsuits Less Hostile but Grassroots Opposition Grows.” *Music & Copyright*, October 29, 2003.

[79] John Schwartz. “Record Industry May Not Subpoena Online Providers.” *NYTimes.com*, December 19, 2003.

[80] Kevin Fitchard. “Verizon Gains Upper Hand in RIAA Subpoena Ruling.” *Telephony*, January 12, 2004.

[81] Mary Madden and Lee Rainie. “Music and Video Downloading Moves Beyond P2P.” Report, Pew Internet & American Life Project, March 23, 2005. www.pewinternet.org/reports.

[82] Mike Harvey. “Single-Mother Digital Pirate Jammie Thomas-Rasset Must Pay $80,000 per Song.” *Sunday*

Times, June 19, 2009. www.thesundaytimes.co.uk.

[83] United States District Court, District of Minnesota. Capitol Records, Inc., et al. v. Jammie Thomas-Rasset, 06-1497 (MJD/LIB) (July 22, 2011).

[84] Denise Lavoie. "Joel Tenenbaum: Jury Awards $675,000 in Boston Music Downloading Case." *Huffington Post,* July 31, 2009. www.huffingtonpost.com.

[85] United States District Court for the District of Massachusetts. Sony BMG Music Entertainment; Warner Bros. Records Inc.; Atlantic Recording Corp.; Arista Records LLC; and UMG Recordings, Inc. v. Joel Tenenbaum, 07cv11446-NG (July 9, 2010).

[86] Fred von Lohmann. "Offering to Distribute = Distribution, Says Court in Elektra v. Barker." Electronic Frontier Foundation, April 1, 2008. www.eff.org.

[87] Fred von Lohmann. "Making Available Is Not Distribution, Says Court in London-Shire v. Doe." Electronic Frontier Foundation, April 2, 2008. www.eff.org.

[88] Fred von Lohmann. "Big Victory in Atlantic v. Howell: Court Rejects RIAA 'Making Available' Theory." Electronic Frontier Foundation, April 29, 2008. www.eff.org.

[89] John Borland. "Judge: File-Swapping Tools Are Legal." CNet News (Web site), April 25, 2003. news.cnet.com.

[90] Supreme Court of the United States. Metro-Goldwyn-Mayer Studios Inc. et al. v. Grokster, Ltd., et al., 545 US (June 27, 2005).

[91] John Borland. "Last Waltz for Grokster." CNet News (Web site), November 7, 2005. news.cnet.com.

[92] Clive Thompson. "The BitTorrent Effect." *Wired*, p. 150, January 2005.

[93] Krysten Crawford. "BitTorrent as Friend, Not Foe." CNN.com, April 30, 2005.

[94] "Authorities Strike Back at 'Star Wars' Pirates." Associated Press, May 25, 2005.

[95] Jenny Stiernstedt, Astrid E. Johansson, and Fredrik Söderling. Translated by Oliver Grassman. "The Pirate Bay Sentenced to One Year in Prison." *Kultur & Nöje* (Sweden), April 17, 2009. www.dn.se.

[96] David Sarno. “The Internet Sure Loves Its Outlaws.” *Los Angeles Times*, April 29, 2007.

[97] “Police Cleared of Wrongdoing in Pirate Bay Raid.” *Local* (Sweden), April 2, 2007. www.thelocal.se.

[98] Nate Anderson. “Pirate Bay on IFPI Lawsuit: Labels Can ‘Go Screw Themselves.’” Ars Technica (Web site), April 1, 2008. arstechnica.com.

[99] Associated Press. “Swedish Court Upholds Convictions in File-Sharing Case.” *New York Times*, November 26, 2010. www.nytimes.com.

[100] “‘Operation In Our Sites’ Targets Internet Movie Pirates.” US Department of Homeland Security, June 30, 2010. www.ice.gov.

[101] “Operation In Our Sites Protects American Online Shoppers, Cracks Down on Counterfeiters.” US Department of Homeland Security, November 28, 2011. www.ice.gov.

[102] United States District Court for the Eastern District of Virginia. United States of America v. Kim Dotcom et al., [2012] NZHC 2076 (January 5, 2012).

[103] Geoffrey A. Fowler, Devlin Barrett, and Sam Schechner. “US Shuts Offshore File-Share ‘Locker.’” *Wall Street*

Journal, January 20, 2012.

[104] Chloe Albanesius. "After Megaupload, FileSonic Disables File Sharing." *PC Magazine*, January 23, 2012.

[105] Nate Lanxon. "FileSonic, FileServe Pull Fire-Sharing Services Following Megaupload Arrests." *Wired.co.uk*, January 23, 2012. wired.co.uk.

[106] Christopher Kauffman. Private communication, March 2015.

[107] Shelley Hepworth. "Streaming Spells the End of the 'Ownership Era of Music' but Are We Ready to Let Go?" *Guardian,* February 1, 2020. https://www.theguardian.com/music/2020/feb/02/streaming-spells-the-end- of-the-ownership-era-of-music-but-are-we-ready-to-let-go.

[108] IFPI. "IFPI Global Music Report 2023." Accessed July 10, 2023. https://globalmusicreport.ifpi.org/.

[109] Julia Stoll. "SVOD Service Users Shares in the U.S. 2015-2022." *Statista,* October 14, 2022. www.statista.com.

[110] US District Court for the Northern District of California. Oracle America, Inc., v. Google Inc., 872 F.Supp.2d 974 (May 31, 2012).

[111] US Court of Appeals, Federal Circuit. Oracle America, Inc., v. Google Inc., 750 F.3d 1339 (May 9, 2014).

[112] Joe Mullin. "Google Beats Oracle—Android Makes 'Fair Use' of Java APIs." Ars Technica (Web site), May 26, 2016. www.arstechnica.com.

[113] US Court of Appeals for the Federal Circuit. Oracle America, Inc., v. Google LLC. 2017-1118, 2017-1202 (March 27, 2018).

[114] Daniel A. Tysver. "The History of Software Patents: From Benson and Diehr to State Street and Bilski." BitLaw (Web site). Accessed August 14, 2011. www.bitlaw.com.

[115] Rob Tiller. "The PTO Addresses Bilski and Software Patents." Opensource.com, September 30, 2010. opensource.com.

[116] "Microsoft Patent Portfolio Tops IT Industry Scorecards." Microsoft News Center, January 28, 2008. www.microsoft.com.

[**117**] Michael Kanellos. “Patent Auctions: Lawyer’s Dream or Way of the Future?” *ZDNet News*, March 3, 2006. web.archive.org.

[**118**] Matthew Sag and Kurt Rohde. “Patent Reform and Differential Policy.” Northwestern Law & Econ Research Paper No. 925722, Chicago, IL, August 21, 2006. papers.ssrn.com.

[**119**] Barrie McKenna, Paul Waldie, and Simon Avery. “Patently Absurd.” *Globe and Mail*, February 21, 2006. www.theglobeandmail.com.

[**120**] Rob Kelley. “BlackBerry Maker, NTP Ink $612 Million Settlement.” *CNNMoney*, March 3, 2006. money.cnn.com.

[**121**] Charles Duhigg and Steve Lohr. “The Patent, Used as a Sword.” *New York Times*, October 7, 2012. www.nytimes.com.

[**122**] Larry Downes. “The Bilski Case and the Future of Software Patents.” *Center for Internet and Society*, November 11, 2009. cyberlaw.stanford.edu.

[**123**] Nilay Patel. “Nokia vs. Apple: The In-Depth Analysis.” *Engadget* (blog), October 29, 2009. www.engadget.com.

[**124**] Nilay Patel. "Apple Countersues Nokia for Infringing 13 Patents." *Engadget* (blog), December 11, 2009. www.engadget.com.

[**125**] US District Court, Northern District of California. Apple Inc. v. Samsung Electronics Co. et al., CV 11 1846 LB (April 15, 2011).

[**126**] Florian Mueller. "Apple Seeks $2.5 Billion in Damages from Samsung, Offers Half a Cent per Standard-Essential Patent." *Foss Patents* (blog), July 24, 2012. www.fosspatents.com.

[**127**] Kurt Eichenwald. "The Great Smartphone War." *Vanity Fair*, June 2014.

[**128**] Nilay Patel. "Slide to Unlock: How Apple's Patents Are Changing Android." *Verge*, March 6, 2012. www.theverge.com.

[**129**] Matt Rosoff. "The Smartphone Patent Wars Are Finally Coming to an End." *Business Insider*, December 23, 2014. www.businessinsider.com.

[**130**] Lance Whitney. "Samsung Willing to Pay Apple $548M over Patent Claims, but Fight Drags On." CNet News (Web site), December 4, 2015. www.cnet.com.

[131] Malcolm Owen. “Samsung Owes Apple $539M for Infringing on iPhone Patents, Jury Finds.” Apple Insider (Web site), May 24, 2018. appleinsider.com.

[132] Supreme Court of the United States. Alice Corporation Pty. Ltd. v. CLS Bank International, 573 US __, Docket No. 13-298 (June 19, 2014).

[133] The United States Patent and Trademark Office. “2106 Patent Subject Matter Eligibility [R-08.2017].” January 24, 2018. Accessed March 27, 2018. www.uspto.gov/web/offices/pac/mpep/s2106.html.

[134] Robert L. Maier. “Will Any Software Patents Survive?” *New York Law Journal*, November 21, 2017. www.law.com/newyorklawjournal/.

[135] Joe Mullin. “East Texas Judge Throws Out 168 Patent Cases in One Fell Swoop.” Ars Technica (Web site), October 1, 2015. artstechnical.com.

[136] United States District Court for the Eastern District of Texas, Marshall Division. Edekka LLC v. 3Balls.com, Inc., et al. 2:15-CV-585 JRG (September 21, 2015).

[137] Robert R. Sachs. “One Year Anniversary: The Aftermath of #Alicestorm.” *Bilskiblog: Analysis and*

Commentary on Patent Eligibility and Patent Strategy, June 20, 2015. www.bilskiblog.com.

[138] Fenwick and West Intellectual Property Group. "Two Years After Alice: A Survey of the Impact of a 'Minor Case.'" *Bilskiblog: Analysis and Commentary on Patent Eligibility and Patent Strategy*, June 16, 2016. www.bilskiblog.com.

[139] United States Court of Appeals for the Federal Circuit. Richard A. Williamson v. Citrix Online, LLC, et al. 792 F. 3d 1339 (June 16, 2015).

[140] Paula Samuelson. "Legally Speaking: Software Patents Are Falling Down." *Communications of the ACM*, Vol 58(11), pp. 27–29, November 2015.

[141] Helen Nissenbaum. "Should I Copy My Neighbor's Software?" In *Computers, Ethics, & Social Values*, edited by Deborah G. Johnson and Helen Nissenbaum. Prentice Hall, Englewood Cliffs, NJ, 1995.

[142] "A Brief History of Software Licensing." Licenseware (Web site), January 16, 2023. https://licenseware.io/a-brief-history-of-software-licensing/.

[143] Richard P. Stallman. "Why Software Should Not Have Owners." GNU Project Web server, June 17, 2003.

www.gnu.org/philosophy/why-free.html.

[144] "The Open Source Definition." Open Source Initiative, 2003. www.opensource.org/docs/definition.php.

[145] Carolyn A. Kenwood. "A Business Case Study of Open Source Software." Technical report, MITRE Corporation, Bedford, MA, July 2001.

[146] Andrew Leonard. "Let My Software Go!" *Salon* (Web site), April 14, 1998. www.salon.com.

[147] "Mobile Operating System Market Share Worldwide: June 2022–June 2023." StatCounter. Accessed July 10, 2023. gs.statcounter.com.

[148] "Browser Market Share Worldwide: June 2022–June 2023." Statcounter. Accessed July 10, 2023. gs.statcounter.com.

[149] Stephen Shankland. "Study Lauds Open-Source Code Quality." CNet News (Web site), February 19, 2003. news.cnet.com.

[150] Richard P. Stallman. "Linux and the GNU Project." GNU Project Web server, December 14, 2002. www.gnu.org/gnu/linux-and-gnu.html.

[151] Sean Michael Kerner. “LinuxCon Analysts: Linux Is Winning.” *Datamation*, August 12, 2010. www.datamation.com.

[152] Thomas Alsop. “Distribution of the Top 500 Supercomputers Worldwide 2017-2022, by OS.” Statista, February 27, 2023. www.statista.com.

[153] Creative Commons, Stanford Law School. *Get Creative* (movie), 2002. www.creativecommons.org.

[154] Lawrence Lessig. *The Future of Ideas: The Fate of the Commons in a Connected World*. Random House, New York, NY, 2001.

[155] “Explore / Creative Commons.” Flickr (Web site). Accessed July 10, 2023. www.flickr.com/creativecommons/.

Chapter 5

Information Privacy

5.1 Introduction

DO YOU WANT TO KNOW WHERE I LIVE? IF YOU VISIT THE THATSTHEM.COM Web site and type in my name and city, it returns a page giving my address. Type the address you just learned from ThatsThem.com into Google Maps, and it will show you a map of my neighborhood and a view of my house from the street.

Spend a few seconds more, and you can learn a lot about my standard of living. Go to Zillow.com and enter my address. Zillow dutifully returns the estimated value of my house, based on public records that document its size and assessed value.

If you become a friend of one of my friends on Facebook, you can get even more glimpses into my personal life by viewing photos of me that other people have posted and tagged. You can see me lounging by a swimming pool at a family reunion, juggling croquet balls, unwrapping a Christmas present, and walking my daughter Shauna down the aisle on her wedding day.

Scott McNealy, former CEO of Sun Microsystems, caused quite a stir when he said, “You have zero privacy anyway.

Get over it" [1]. You can't deny that computers, databases, and the Internet have made it easier than ever to get lots of information about total strangers. Still, many of us would like to think that we can keep some things private.

A woman in Portland, Oregon, was incredulous when an employee of her husband called from Seattle to tell her he had received a message containing an audio recording of a conversation from inside her house. She and her husband didn't believe the employee until he correctly related details of their conversation about hardwood floors. It turns out the private conversation had been sent by an Amazon Echo personal assistant, which had mistakenly determined that someone had said "Alexa," mistakenly heard a "send message" request, mistakenly heard the name of the employee in her husband's phone's contacts list as the person to whom the message was supposed to be sent, and mistakenly heard the confirmation word "right" when it asked if it had the correct recipient of the message [2].

Is it possible to maintain privacy in the Information Age? In this chapter we focus on privacy issues related to the introduction of information technology. We begin by taking a philosophical look at privacy. What is privacy exactly? Do we have a natural right to privacy in the same way that we

have the right to own property and the right to liberty? What about our need to know enough about others so that we can trust them? How do we handle conflicts between the right to privacy and the right to free expression?

We then survey some of the ways that we leave an "electronic trail" of information behind us as we go about our daily lives. Both private organizations and governments construct databases documenting our activities.

Next, we take a look at data mining, an important tool for building profiles of individuals and communities. Companies use data mining to improve service and target product marketing to the right consumers. Data brokers collect massive amounts of information about individuals and produce mailing lists for direct marketers.

Sometimes corporations push on the borders of personal privacy a little too hard; we look at a few examples where they have had to retreat because of a consumer or political backlash.

5.2 Perspectives on Privacy

In this section we explore what the word “privacy” means, survey some positive and negative consequences of granting people privacy, and discuss whether privacy is a natural right, like the right to life.

5.2.1 Defining Privacy

Philosophers struggle to define privacy. Discussions about privacy revolve around the notion of *access*, where access means either physical proximity to a person or knowledge about that person. There is a tug-of-war between the desires, rights, and responsibilities of a person who wants to restrict access to himself, and the desires, rights, and responsibilities of outsiders to gain access.

From the point of view of an individual seeking to restrict access, privacy is a “zone of inaccessibility” that surrounds a person [3]. You have privacy to the extent that you can control who is allowed into your zone of inaccessibility. For example, you exercise your privacy when you lock the door

behind you when using the toilet. You also exercise your privacy when you choose not to tell your parent the name of the person you are dating. However, privacy is not the same thing as being alone. Two people can have a private relationship. It might be a physical relationship, in which each person lets the other person become physically close while excluding others, or it might be an intellectual relationship, in which they exchange texts containing private thoughts.

When we look at privacy from the point of view of outsiders seeking access, the discussion revolves around where to draw the line between what is private and what is public (known to all). Stepping over this line and violating someone's privacy is an affront to that person's dignity [4]. For example, suppose a friend invites you to see a cool movie trailer available on the Web. You follow them into the computer lab. They sit down at an available computer and begin to type in their login name and password. While it is their responsibility to keep their password confidential, it is also generally accepted that you ought to avert your eyes when someone is typing in their password. Another person's password is not something that you are supposed to know.

On the other hand, society can be harmed if individuals have too much privacy. Suppose a group of wealthy people of the same racial, ethnic, and religious background forms a private club. The members of the club share information with each other that is not available to the general public. If the club facilitates business deals among its members, it may give them an unfair advantage over others in the community who are just as capable of fulfilling the contracts. In this way, privacy can encourage social and economic inequities, and the public at large might benefit if the group had less privacy (or its membership were more diverse).

Here is another example of a public/private conflict, but this one focuses on the privacy of an individual. Most of us distinguish between a person's "private life" (what they do at home) and their "public life" (what they do at work). In general, we may agree that people have the right to keep outsiders from knowing what they do away from work. However, suppose a journalist learns that a wealthy candidate for high public office has lost millions of dollars gambling in Las Vegas. Does the public interest outweigh the politician's desire for privacy in this case?

In summary, privacy is a social arrangement that allows individuals to have some level of control over who is able to

gain access to their physical selves and their personal information.

5.2.2 Harms and Benefits of Privacy

A little reflection reveals that privacy can have both harmful and beneficial consequences.

Harms of Privacy

Giving people privacy can result in harm to society. Some people take advantage of privacy to plan and carry out illegal or immoral activities. Most wrongdoing takes place under the cover of privacy [5].

Some commentators suggest that increasing privacy has caused unhappiness by putting too great a burden on the nuclear family to care for all of its members. In the past people received moral support not just from their immediate family but also from other relatives and neighbors. Today, by contrast, in some cultures, families are expected to solve their own problems, which puts a great strain on some individuals [6].

On a related note, family violence leads to much pain and suffering in some societies. Often, outsiders do not even acknowledge that a family is dysfunctional until one of its members is seriously injured. One reason dysfunctional families in some societies can maintain the pretense of normality as long as they do is because the culture respects the privacy of each family [7].

Humans are social beings. Most of us seek some engagement with others. Sadly, some people may lack sufficient engagement with others because their community marginalizes or excludes them.

Benefits of Privacy

Socialization and individuation are both necessary steps for a person to reach maturity. Privacy is necessary for a person to blossom as an individual [8].

)

Privacy is the way in which a social group recognizes and communicates to the individual that they are responsible for their development as a unique person, a separate moral agent [9]. Privacy is a recognition of each person's true freedom [10].

Privacy is valuable because it lets us be ourselves. Consider the following example. Imagine someone is in a park playing with their child. How would their behavior be different if they knew someone else was carefully watching them, perhaps even recording them, so that they could tell others about the person's parenting skills? They might well become self-conscious about their behavior. Few people would be able to carry on without any change to their emotional state or physical actions [**11**].

On a similar note, privacy lets us remove our public persona [**12**]. Imagine a sales representative who is having a hard time with one of her company's important clients. At work, she must be polite to the client and scrupulously avoid saying anything negative about the client in front of any coworkers, lest she demoralize them, or even worse, lose her job. In the privacy of her home, she can "blow off steam" by confiding in her spouse, who lends her a sympathetic ear and helps motivate her to get through the tough time at work. If people did not have privacy, they would have to wear their public face at all times, which could be damaging to their psychological health.

Privacy can foster intellectual activities. It allows us to shut out the rest of the world so that we can focus our thoughts

without interruption, be creative, and grow spiritually [**13**, **14**, **15**].

Some maintain that privacy is the only way in which people can develop relationships involving respect, love, friendship, and trust. You can think of privacy as "moral capital" [**16**]. People use this capital to build intimate relationships. Taking away people's privacy means taking away their moral capital. Without moral capital, they have no means to develop close personal relationships.

In order to have different kinds of social relationships with different people, we need to have some kind of control over who knows what about us [**17**]. You can imagine everyone having a "ladder" of privacy [**11**]. At the top of the ladder is the person we share the most information with. For many people, this person is their partner, husband, or wife. As we work our way down the ladder, we encounter people we would share progressively less information with.

Others are critical of suggestions that tie intimacy too closely to sharing information [**9**]. A patient might tell their psychoanalyst things they would not even reveal to their romantic partner, but that does not imply that they experience deeper intimacy with their psychoanalyst than with their partner. Intimacy is not just about sharing

information; it's also about caring. The mutual caring that characterizes a healthy life partnership results in a greater level of intimacy than can be gained simply by sharing personal information.

Summary

To summarize our discussion, allowing people to have some privacy has a variety of beneficial effects. Granting people privacy is one way that society recognizes them as adults and indicates they are responsible for their own moral behavior. Privacy helps people to develop as individuals and to truly be themselves. It provides people the opportunity to shut out the world, be more creative, and develop spiritually. It allows each of us to create different kinds of relationships with different people.

Privacy also has numerous harmful effects. It provides people with a way of covering up actions that are immoral or illegal. If a society sends a message that certain kinds of information must be kept private, some people caught in abusive or dysfunctional relationships may feel trapped and unable to ask others for help.

Weighing these benefits and harms, we conclude that granting people at least some privacy is better than denying

people any privacy at all. That leads us to our next question: Is privacy a natural right, like the right to life?

5.2.3 Is There a Natural Right to Privacy?

Most of us agree that every person has certain natural rights, such as the right to life, the right to liberty, and the right to own property. Many people also talk about our right to privacy. Is this a natural right as well?

Privacy Rights Evolve from Property Rights

People's belief in a right to privacy may have grown out of their property rights [8]. For example, historically, Europeans have viewed the home as a sanctuary. The English common-law tradition has been that “a man’s home is his castle.” No one—not even the king—can enter without permission, unless there is probable cause of criminal activity.

In 1765 the British Parliament passed the Quartering Act, which required American colonies to provide British soldiers with accommodations in taverns, inns, and unoccupied buildings. After the Boston Tea Party of 1773, the British Parliament attempted to restore order in the colonies by

passing the Coercive Acts. One of these acts amended the Quartering Act to allow the billeting of soldiers in private homes, breaking the centuries-old common-law tradition and infuriating many colonists. It's not surprising, then, that Americans restored the principle of home as sanctuary in the Bill of Rights.

Third Amendment to the United States Constitution

> No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

In certain villages in the Basque region of Spain, each house is named after the person who originally constructed it. Villagers refer to people by their house names, even if the family living in the house has no relation to the family originally dwelling there.

These examples show a strong link between a person and their property. From this viewpoint, privacy is seen in terms of control over personal territory, and privacy rights evolve out of property rights.

Warren and Brandeis: Clearly, People Have a Right to Privacy

We can see this evolution laid out in a highly influential paper, published in 1890, by Samuel Warren and Louis Brandeis. Samuel Warren was a Harvard-educated lawyer who became a businessman when he inherited a paper manufacturing business. His wife was the daughter of a US senator and a leading socialite in Boston. Her parties attracted the upper crust of Boston society. They also attracted the attention of the *Saturday Evening Gazette*, a tabloid that delighted in shocking its readers with lurid details about the lives of the Boston Brahmins.[1] Fuming at the paper's coverage of his daughter's wedding, Warren enlisted the aid of Harvard classmate Louis Brandeis, a highly successful Boston attorney (and future US Supreme Court justice). Together Warren and Brandeis published an article in the *Harvard Law Review* called "The Right to Privacy" [18]. In their highly influential paper, Warren and Brandeis argue that political, social, and economic changes demand

recognition for new kinds of legal rights. In particular, they write that it is clear that people in modern society have a right to privacy and that this right ought to be respected. To make their case, they focus on—as you might have guessed—abuses in newspapers.

According to Warren and Brandeis:

> **The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy the prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. . . . The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. [18, p. 196]**

Meanwhile, Warren and Brandeis argue, there are no adequate legal remedies available to the victims. Laws against

libel and slander are not sufficient because they do not address the situation where malicious but true stories about someone are circulated. Laws addressing property rights also fall short because they assume people have control over the ways in which information about them is revealed. However, cameras and other devices are capable of capturing information about a person without that person's consent (Figure 5.1).

Figure 5.1

Warren and Brandeis argued that the legal system should protect people's "right to be let alone."

(PhamousFotos/Splash News/Newscom)

Warren and Brandeis pointed out that the right to privacy had already been recognized by French law. They urged the American legal system to recognize the right to privacy, which they called "the right to be let alone" [18]. Their

reasoning was highly influential. Though it took decades, the right to privacy is now recognized in courts across America [19].

Thomson: Every "Privacy Right" Violation Is a Violation of Another Right

Judith Jarvis Thomson has a completely different view about a right to privacy. She writes: "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is" [20]. Thomson points out problems with defining privacy as "the right to be let alone," as Warren and Brandeis have done. In some respects, this definition of privacy is too narrow. Suppose the police use an X-ray device and supersensitive microphones to monitor the movements and conversations of Smith in their home. The police have not touched Smith or even come close to them. They have no knowledge they are monitoring them. The police have let Smith alone, yet people who believe in a right to privacy would surely argue that they have violated Smith's privacy. In other respects, the definition of privacy as "the right to be let alone" is too broad. If I hit Jones on the head with a brick, I have not let them alone, but it is not their right of privacy I have violated—it is their right to be secure in their own person.

Thomson argues that whenever the right to privacy is violated, another right is violated as well. For example, suppose a man owns a pornographic picture. He doesn't want anyone else to know he owns it, so he keeps it in a wall safe. He removes it from his safe only when he has taken steps to prevent others from looking into his home. Suppose we use an X-ray machine to look into his home safe and view the picture. We have violated his privacy, but we have also violated one of his property rights—the right to decide who (if anybody) sees the picture.

Here is another example. Suppose a Saudi Arabian woman wishes to keep her face covered for religious reasons. When she goes out in public, she wears a niqab (face veil). If I should walk up and pull away her niqab to see her face, I have violated her privacy. But I have also violated her right to observe religious and cultural customs, as well as one of her rights over her person—to decide who should touch her.

According to Thomson, there is a cluster of rights associated with privacy, just as there is a cluster of rights associated with property and a cluster of rights associated with our physical selves. In Thomson's view, every violation of a privacy right is also a violation of a right in some other cluster. Since this is the case, there is no need to define

privacy precisely or to decide exactly where to draw the line between violations of privacy and acceptable conduct.

Autonomous Moral Agents Need Some Privacy

Thomson is not alone in disputing that privacy is a natural right. Many philosophers think privacy principles should be based on the more fundamental principle that each person is worthy of respect [10]. We give each other privacy because we recognize privacy is needed if people are to be autonomous moral agents able to develop healthy personal relationships and act as free citizens in a democratic society.

Jeffrey Reiman supports this view:

> **The right to privacy protects the individual's interest in becoming, being, and remaining a person. It is thus a right which *all* human individuals possess—even those in solitary confinement. It does not assert a right never to be seen even on a crowded street. It is sufficient that I can control whether and by whom my body is experienced in some significant places and that I have the real possibility of repairing to those places. It is a right which protects my capacity to enter into intimate relations, not because it protects my reserve of generally withheld information, but because it enables me to make the commitment that underlies caring as *my***

> **commitment uniquely conveyed by *my* thoughts and witnessed by *my* actions. [9, p. 314]**

Note Reiman's fairly restricted view of privacy. He carefully points out areas where privacy is necessary. He does not argue that privacy is a natural right, nor does he suggest that a person has complete control over what is held private.

Conclusion: Privacy Is a Prudential Right

In conclusion, philosophers disagree whether there is a natural right to privacy, but most commentators can agree that privacy is a **prudential right**. That means rational agents would agree to recognize some privacy rights because granting these rights is to the benefit of society [21].

5.2.4 Privacy and Trust

While many people complain about threats to privacy, it is clear upon reflection that in some important ways people in many cultures have more privacy than their ancestors did [22]. Only a couple of centuries ago, societies were agrarian. People lived with their extended families in small homes. The nearest community center was the village, where everyone

knew everyone else and people took a keen interest in each other's business. In many places, organized religion played an important role in everyday life. In this kind of society, there was a strong pressure to conform [**12**]. There was greater emphasis on the community and lesser emphasis on the individual.

Some modern cultures foster much greater privacy. Prosperity, the single-family home, the automobile, television, and computers have contributed to many people's privacy. The single family home gives physical separation from other people. The automobile allows solitary travel instead of public transport. The television brings entertainment inside the home, taking many people out of the neighborhood movie theater. With a computer and an Internet connection, information can be accessed at home rather than by visiting the public library [**11**]. These are just a few examples of ways in which modern conveniences allow people to spend time by themselves or in the company of a few family members or friends.

In the past, many young people lived at home with their parents until they were married. Today many young unmarried adults live autonomously. This lifestyle provides them with previously unthought-of freedom and privacy [**22**].

The consequence of all this privacy is that we live among strangers. Many people know little more about their neighbors than their names (if that). Yet when we live in a society with others, we must be able to trust them to some extent. How do we know that a taxi driver will get us where we want to go without harming us? How do parents and caregivers know they can trust the people who have charge of their children? How does the bank know that, if it loans someone money, it will be repaid?

In order to trust others, we must rely on their reputations. This was easier in the past, when people didn't move around so much and everyone knew everyone else's history. Today society must get information out of people to establish reputations. One way of getting information from a person is through an **ordeal**, such as a lie detector test or a drug test. The other way to learn more about individuals is to issue (and request) **credentials**, such as a driver's license, key, employee badge, credit card, college degree, or online rating [22].

5.2.5 Case Study: The New Parents

Meena and Alex are the proud parents of a new baby. They had begun exploring options for child care from the beginning of the pregnancy because both of them have full-time and highly satisfying careers in the computer field. They visited numerous day-care facilities, but the ones they liked the best had no openings. For this reason, they decided to hire a personal nanny, even though it was more expensive. After their baby was born, Meena spent three months at home on maternity leave. During this time, the parents interviewed a half dozen nannies and hired one after carefully checking their references.

Just before the nanny was due to start work, Meena and Alex had coffee with a few of their friends who are all parents or caregivers of young children. The friends tell horror stories about abusive nannies, and they all recommend a software program called LiveSecurityWatch. Meena and Alex purchase LiveSecurityWatch and install it on a laptop computer placed in the family room. With the system in place, they can use their workplace computers to see and hear how the nanny interacts with their baby. The nanny has no idea that the family's computer is being used as a surveillance system.

Is it wrong for Meena and Alex to secretly monitor the behavior of their baby's nanny?

Rule-Utilitarian Evaluation

If all parents monitored their nannies or child-care providers and took actions when warranted, such as firing nannies who did not perform well, it is unlikely such monitoring would remain a secret for long. Under these circumstances, nannies would be much more careful to be on their best behavior. This would potentially have the long-term effects of reducing the instances of child abuse and increasing the peace of mind of parents. On the other hand, the harms of the monitoring would be significant in terms of increasing the stress and reducing the job satisfaction of nannies and child-care providers. After all, who wants to be monitored constantly? These negative aspects of the job could lead to an increased turnover rate of nannies. Less experienced nannies might well provide lower-quality care to the babies they tend. The harms of having all parents monitoring their nannies or child-care providers appear to be greater than the benefits. Hence we conclude it is wrong for Meena and Alex to secretly monitor their nanny.

Social-Contract-Theory Evaluation

Social contract theory emphasizes the adoption of rules that rational people would agree to accept because they are to everyone's mutual benefit, as long as everyone else follows

the rules as well. As we discussed earlier in this section, privacy is a prudential right. It is reasonable for society to give privacy to people in their own homes, and it is also reasonable for family members within each home to give each other some privacy as well. The nanny wouldn't expect her interactions with the baby in a park or a grocery store to be private, but it is reasonable for her to expect privacy when taking care of the baby inside the home. Hence Meena and Alex's decision to secretly monitor the nanny was wrong because it violated her right to privacy.

Kantian Evaluation

Let's consider the morality of acting according to the following rule: "An employer may secretly monitor the work of an employee who works with vulnerable people." To evaluate the rule using the first formulation of the Categorical Imperative, we universalize it. What would happen if every employer secretly monitored the work of employees who worked with vulnerable people? If that were the case, then employees who worked with vulnerable populations would have no expectation of privacy, and it would be impossible for employers to secretly monitor their work. Hence the proposed rule is self-defeating, and it would be wrong to act according to this rule.

We can also evaluate this situation using the second formulation of the Categorical Imperative. As parents, Meena and Alex are responsible for the well-being of their baby. In order to be more confident that their baby is safe in the care of the nanny, they choose to secretly observe the behavior of the nanny. The observation is the means to their desired end of having their baby well cared for. The nanny naturally assumes that her interactions with the baby inside the residence are private. By not disclosing to the nanny the fact that she is being watched remotely, Meena and Alex have treated the nanny as a means to an end. Hence the action of Meena and Alex is wrong.

Virtue-Ethics Evaluation

As parents, Meena and Alex are ultimately responsible for the well-being of their child. Rather than put their baby in a day-care facility they considered to be second-rate, they decided to spend more money and hire a personal nanny. That action is characteristic of good parents who put their children's needs before their own. When Meena and Alex heard about abusive nannies, it is only natural that they would become worried about their child's welfare, particularly because babies are defenseless and unable to communicate. According to virtue theory, parents should be

partial toward their children. We can view Meena and Alex's decision to use the webcam as an action characteristic of good parents. However, we would also expect that once Meena and Alex are reassured they hired a fine nanny who is taking good care of their infant, they would trust the nanny and discontinue the secret monitoring.

From the points of view of rule utilitarianism, social contract theory, and Kantianism, we have concluded that it is wrong for Meena and Alex to secretly monitor how well their nanny takes care of their baby. However, from the perspective of virtue ethics, the action of Meena and Alex is morally acceptable because it is consistent with parents of good character.

o learn more about the Boston Brahmins, consult *Wikipedia* ww.wikipedia.org).

5.3 Information Disclosures

5.3.1 Public Records

As we go about our lives, we leave behind an electronic trail of our activities, thanks to computerized databases. Some events result in the creation of public records. A **public record** contains information about an incident or action reported to a government agency for the purpose of informing the public [23]. Examples of public records are birth certificates, marriage licenses, motor vehicle records, criminal records, deeds to property, and the salaries of state employees (including your professor, if you are studying at a public institution). Making government records public is one way to hold government agencies accountable for their actions and help ensure that all citizens are being treated fairly.

When public records were written on paper and kept in county courthouse basements, they were relatively hard to retrieve. Computerized databases and the Internet have made accessing many public records quick and inexpensive, and

there are a lot of good purposes to which we can put all that information. Before a school hires a teacher, it can check the candidate's criminal record to ensure there are no convictions for child abuse. Before a transit system hires a bus driver, it can check the applicant's driving record. Before moving to a new city, you can check out the crime rate of the neighborhood you're interested in.

Other uses of public records may not be as laudable. Thanks to information technology, it's easier than ever to learn a lot about someone's wealth. For most people, their home is their principal asset. But we saw above that anyone with Internet access can visit Zillow.com, type in the address of someone's house, and quickly learn Zillow's estimate of the house's worth, based on information about the size of the house (a public record), the selling price of the house (a public record), and recent sales of similar houses in the neighborhood (also public records).

5.3.2 Information Held by Private Organizations

Private organizations, too, maintain extensive records of our activities. Databases store information about the purchases we make with our credit cards, the groceries we buy at a

discount with our loyalty cards, the calls we make with our cell phones, and much more. The companies collecting this information use it to bill us. They may also use this information to serve us better. For example, Amazon uses information about book purchases to build profiles of its customers. With a customer profile, Amazon can recommend other books the customer may be interested in buying. On the other hand, companies may share information about our purchases with other companies that then send us junk mail for products they hope to sell us.

Often people voluntarily disclose information to private organizations. Product registration forms and contest entries often ask consumers to reveal a great deal of personal information. I once received a product preference survey from Procter & Gamble; it said, in part:

> **Your opinions matter to us. That's why we've selected you to participate in one of the most important consumer research surveys we'll do this year. Whether or not you have completed one of our surveys in the past, you can help us continue to create the products that meet your needs. Simply answer the following questions, provide your name and address, and mail it back to us.**

> **That way, we will be able to contact you if there are any special offers that might be of interest to you.**

The questionnaire asked about my family's use of nasal inhalants, coffee, peanut butter, orange juice, laundry detergent, fabric softener, household cleaner, deodorant, toothpaste, detergents, skin-care and hair-care products, cosmetics, mouthwash, diapers, laxatives, and disposable briefs. It provided a list of 60 leisure activities, ranging from various sports to travel to gambling, and asked me to choose the three activities most important to my family. It also asked my date of birth, the sex and age of everyone living in my home, my occupation, the credit cards we used, and our annual family income. If I had returned the questionnaire (which I didn't), Procter & Gamble would have been free to use this information any way it wished.

Many of us voluntarily share information about our activities by posting messages and uploading photos to social network sites like Facebook. These sites make it easy to communicate with many friends and acquaintances at once, but this information can be put to other purposes as well [**24**]. Social Intelligence Corporation provides employers with background checks on potential employees by searching the

Internet for posts and photos by the job candidates that reveal negative activities specified by the employer, such as "racist remarks or activities, sexually explicit photos or videos, and illegal activity such as drug use" [25].

Recall the perspective that privacy is a "zone of inaccessability." Using this definition, we can say that our personal information is private to the extent that we can control who has access to it. In some settings we expect to have much more control over our personal information than in other venues. For example, we have much more control over who takes our picture when we're at home than when we're at a football game. Hence our expectations about the privacy of our personal information depend on the situation. In the rest of this section, we survey a variety of ways in which private organizations collect and use personal information, starting with situations in which most of us would assume we have less privacy and finishing with situations in which we would expect to have much more privacy.

5.3.3 Facebook Tags

In the Facebook social network, a **tag** is a label identifying a person in a photo. When you post a photo to Facebook, you

can tag the people in the photo who are on your list of Facebook friends. In a similar way, any of your Facebook friends can tag you in photos they post to the site. People tag photos in Facebook an average of 100 million times per day [26].

In December 2010, Facebook introduced a new time-saving feature called Tag Suggestions. When a Facebook user added a new photo, Facebook used facial recognition software to suggest the name of the friend appearing in the photo. In June 2011, the Electronic Privacy Information Center (EPIC) filed a complaint about Facebook Tag Suggestions with the Federal Trade Commission [27]. EPIC claimed that in order to develop its facial recognition technology, Facebook gathered facial data from users' photos without their consent. Others raised the concern that the introduction of an automatic tagging feature would increase the chance that photos would be improperly tagged, which could cause a problem if the photos were not complimentary [28].

5.3.4 Enhanced 911 Services

All cell phone providers in the United States are required by law to be able to track the locations of active cell phone users

to within 100 meters. The safety benefit of this capability is obvious. Emergency response teams can reach people in distress who have dialed 911, even if they are unable to speak or do not know exactly where they are.

The ability to identify the location of active cell phone users has other benefits. For example, it makes it easier for cell phone companies to identify where signal strength is weak and coverage needs to be improved.

The downside of enhanced 911 service is a potential loss of privacy. Because it is possible to track the location of active cell phone users, what happens if information is sold or shared? Suppose you call your employer and tell him you are too sick to come into work. Your boss is suspicious, since this is the third Friday this summer you've called in sick. Your employer pays your cell phone provider and discovers that you made your call from out of town [29].

5.3.5 Rewards or Loyalty Programs

Rewards or loyalty programs for shoppers have been around for more than 100 years. One example is S&H Green Stamps, the most popular rewards program in the United

States from the 1950s through the 1970s. Shoppers would collect Green Stamps with purchases, paste them into booklets, and redeem the booklets by shopping in the Sperry & Hutchinson catalog for household items.

Today many shoppers take advantage of rewards programs sponsored by grocery stores. Card-carrying members of the store's "club" save money on many of their purchases, either through coupons or instant discounts at the cash register. The most significant difference between the Green Stamps program and a contemporary shopper's club is that today's rewards programs are run by computers that record every purchase. Companies can use information about the buying habits of particular customers to provide them with individualized service.

For example, ShopRite grocery stores have computerized shopping carts. The shopping cart has a card reader and an LCD screen. Customers identify themselves by swiping their loyalty card through the card reader. A computer taps into a database with the customer's buying history and uses this information to guide the customer to frequently purchased products. As the cart passes through the aisles, pop-up ads display items the computer predicts the customer may be interested in purchasing [30].

)

Critics of grocery club cards say that the problem is not that card users pay less for their groceries but that those who don't use cards pay more. They give examples of club-member prices being equivalent to the regular product price at stores without customer loyalty programs [**31**].

Some consumers respond to the potential loss of privacy by giving phony personal information when they apply for these cards. Others take it a step further by regularly exchanging their cards with those held by other people [**32**].

Other consumers have learned how to "game" the system. One shopper noticed that by alternating her ground coffee purchases between Starbucks brand and Dunkin' Donuts brand, she got better prices than when she just bought Starbucks [**33**].

5.3.6 Body Scanners

(This section describes scanners designed to take a person's measurements. Advanced imaging technology scanners used at airport security checkpoints are discussed in Section 6.11.4.)

Looking good is important to many, if not most, of us. Computer technology is making it possible for us to save time

shopping and find clothes that fit us better (Figure 5.2).

Figure 5.2

A computer takes a customer's measurements.
(Richard Drew/AP Images)

In some stores in the United Kingdom, you can enter a booth, strip to your undergarments, and be scanned by a computer, which produces a three-dimensional model of your body. The computer uses this information to recommend which pairs of jeans ought to fit you the best. You can then sit in front of a computer screen and preview what various pairs of jeans will look like on you. When you have narrowed down your search to a few particular brands and sizes, you can actually try on the jeans.

Body scans are also being used to produce custom-made clothing. At Brooks Brothers stores in the United States, customers who have been scanned can purchase suits tailored to their particular physiques [34].

5.3.7 RFID Tags

Imagine getting up in the morning, going into the bathroom, and seeing a message on the medicine cabinet's computer screen warning you that your bottle of ibuprofen is close to its expiration date. Later that day you are shopping for a new pair of pants. As you try them on, a screen in the dressing room displays other pieces of clothing that would complement your selection.

These scenarios are possible today thanks to a technology called RFID, short for radio-frequency identification. An RFID is a tiny wireless transmitter. Manufacturers are replacing bar codes with RFIDs because they give more information about the product and are easier to scan. An RFID can contain specific information about the particular item to which it is attached (or embedded), and a scanner can read an RFID from six feet away. When bar codes are replaced by RFIDs, checkouts are quicker and companies track their inventory more accurately (Figure 5.3).

Figure 5.3

Employees take inventory more quickly and make fewer errors when items are marked with RFID tags.

(Marc F. Henning/Alamy Stock Photo)

However, because RFIDs are not turned off when an item is purchased, the new technology has raised privacy concerns. Imagine a workplace full of RFID scanners. A scanner in your cubicle enables a monitoring system to associate you with the tags in your clothes. Another scanner picks up your presence at the water cooler. The next thing you know, your boss has called you in for a heart-to-heart talk about how many breaks you're taking. Some privacy advocates say consumers should have a way to remove or disable RFIDs in the products they purchase [35, 36].

5.3.8 Implanted Chips

In Taiwan, every domesticated dog must contain a microchip implant identifying its owner and residence [37]. The microchip, about the size of a grain of rice, is implanted into the dog's ear using a syringe. When a dog gets lost, the authorities can easily retrieve the address and return the pet to its owner.

Verichip Corporation created an RFID tag approved for use in humans. The company claimed that 2,000 people worldwide had a Verichip implant. The most common reason for getting an implanted RFID chip was to allow doctors to learn about the medical conditions of unconscious patients [38]. However, in some trendy European nightclubs, patrons have used their implanted RFID chips as in-house "debit cards" for purchasing food and drinks [39]. After some highly publicized incidents of abducted or missing children, the media have reported parents ruminating on the idea of implanting microchip tracking devices in their kids [40, 41].

5.3.9 Mobile Apps

It's obvious that Google Maps needs to know your location, but did you know that when you play Angry Birds or use Brightest Flashlight, information about your location is being collected and sold to advertisers and data brokers? These

apps are not unusual. Flurry, a company specializing in analyzing data collected from mobile apps, has access to data from more than a *half million* apps running on most iPhones and Android smartphones, unless people explicitly block them [**42**].

5.3.10 Facebook Login

Facebook Login is popular with software developers because it gives them access to a great deal of information about consumers. Many people use Facebook Login to log into Web sites or apps using their Facebook credentials, because they find it easier than remembering usernames and passwords for every site they visit. However, they may not realize that when they use Facebook Login, they give permission to the app's developer to access a lot of information from their Facebook profile, including their name, location, email address, and friends list [**43**].

5.3.11 OnStar

OnStar Corporation manufactures a communication system incorporated into an automobile's rearview mirror. OnStar provides emergency, security, navigation, and diagnostics services to its subscribers. For example, a driver who runs out

of gas can push the Blue OnStar button to initiate a conversation with an OnStar representative. The driver does not have to know their exact location, because the system automatically sends the GPS location of the automobile to OnStar, which can send help. The driver does not always need to initiate the communication with OnStar representatives. For example, whenever the air bags deploy on an OnStar-equipped vehicle, the system automatically communicates the location of the vehicle to an OnStar center, which can initiate a 911 call.

The capabilities of the OnStar system were dramatically revealed in Visalia, California, in October 2009, when a man with a sawed-off shotgun ordered two occupants of a 2009 Chevrolet Tahoe to get out of their vehicle. He took their money and drove off in the SUV. After the police got the victim's permission to track down the stolen vehicle, OnStar provided the police with its current location. When police cars began to tail the Tahoe, its driver sped up. At this point the OnStar service center issued a command to the SUV that electronically disabled the gas pedal, causing the Tahoe to gradually slow to a halt and allowing the police to apprehend the carjacker. Visalia Police Chief Colleen Mestas complimented the new technology for preventing a potentially dangerous high-speed car chase [**44**].

Because OnStar has the ability to track the location of OnStar-equipped vehicles and listen to conversations happening within them, some privacy advocates have expressed concerns about possible abuses that could occur if this information were shared with law enforcement agencies. For example, suppose the police were looking for suspects in an unsolved crime. Should they have the right to gather information from OnStar about all OnStar-equipped vehicles that were in the area at the time of the crime?

In an hour-long Web chat on the General Motors FastLane site in November 2009, OnStar's Jane Speelman responded to these concerns. According to Speelman, OnStar does not continuously monitor the location of OnStar-equipped vehicles, OnStar does not provide information about the speed of vehicles to law enforcement agencies, and OnStar representatives cannot listen to conversations inside a vehicle without alerting the vehicle's occupants [45].

5.3.12 Automobile "Black Boxes"

You probably know about airplane flight data recorders, also called "black boxes," which provide information useful in

postcrash investigations. Did you know that modern automobiles also come equipped with a "black box"? A microprocessor attached to the car's air bag records information about the speed of the car, the amount of pressure being put on the brake pedal, and whether the seat belts are connected. After a collision, investigators can retrieve the microprocessor from the automobile and view data collected in the five seconds before the accident [**46**].

5.3.13 Medical Records

The change from paper-based to electronic medical records has the potential to lower the costs and improve the quality of medical care by making it quicker and cheaper for information about patients to be shared among nurses, physicians, and other caregivers. The US government has been promoting the conversion to electronic medical records as one way to rein in the rapid increase in health care costs. The Health Information Technology for Economic and Clinical Health (HITECH) Act required doctors and hospitals to move from paper records to electronic records.

However, once an individual's entire medical history is consolidated in a database accessible by many, it can be more difficult to control how that information is disseminated,

with potentially significant consequences. An employer may choose to pass over a job candidate who has had serious medical problems [47]. A woman who has successfully completed a treatment program for drug addiction may be discriminated against if information about her former drug use is revealed.

In November 2003, Florida state law enforcement officials seized the medical records of radio commentator Rush Limbaugh, as part of an investigation to determine whether Limbaugh had illegally obtained prescription pain medications from several doctors. The American Civil Liberties Union filed a friend-of-the-court brief in partial support of Limbaugh, arguing that law enforcement officials acted improperly in obtaining a warrant that allowed them to seize all of Limbaugh's medical records, not just those relevant to the criminal investigation [48].

5.3.14 Digital Video Recorders

TiVo, Inc. is a well-known manufacturer of digital video recorders. TiVo provides a service that lets its subscribers more easily record programs they are interested in watching later. For example, with a single command a subscriber can

instruct the TiVo to record every episode of a TV series. TiVo collects detailed information about the viewing habits of its users. Because the system monitors the activities of the users second by second, its data are more valuable than the information provided by other services. For example, TiVo's records show that 66 percent of the ads shown during primetime on broadcast networks are skipped [**49**].

5.3.15 Cookies

A **cookie** is a file placed on your computer's hard drive by a Web server. The file contains information about your visits to a Web site. Cookies can contain login names and passwords, product preferences, and the contents of virtual shopping carts. Web sites use cookies to provide you with personalized services, such as custom Web pages. Instead of asking you to type in the same information multiple times, a Web site can retrieve that information from a cookie.

The General Data Protection Regulation (GDPR) is a set of rules governing the collection of information from citizens of the European Union. Implemented in May 2018, the GDPR has had an impact on American citizens, too. Among its many provisions, the GDPR requires that companies disclose the information they are seeking to collect and why they are

collecting it, and get permission before gathering the information. In response to the GDPR, most American companies with a multinational presence have adopted new privacy guidelines and have begun displaying banners on their Web pages disclosing that they are using cookies to gather personal information and asking users to indicate their understanding and consent by clicking on a box [50].

5.4 Data Mining

In the previous section we surveyed a few of the many ways that companies collect information on people's daily activities. In this section we look at how this information has itself become a commodity that companies buy and sell in order to provide more personalized services to their existing customers and to target potential customers more accurately.

5.4.1 Data Mining Defined

Before you use a grocery store's loyalty card, you have to spend some time filling out an application that asks for a lot of personal information, such as your name, address, and phone number. After the store has processed your application, using your loyalty card is easy. You just swipe your card or type in your phone number, and the register recognizes you as a customer and gives you the appropriate discounts on your food purchases. At the same time, information about your purchases is entered into a database.

A record in a database records a single transaction, such as a particular item you purchased at the grocery store. A database record is like a single snapshot of a person. It tells

you something about the person, but in isolation its value is limited. **Data mining** is the process of searching through many records in one or more databases looking for patterns or relationships. Data mining is a way to generate new information by combining facts found in multiple transactions, and it can also be a way to predict future events. By drawing upon large numbers of records, data mining allows an organization to build an accurate profile of an individual from a myriad of snapshots.

Google's personalized search and collaborative filtering are two examples of how companies are using data mining to create more personal relationships with their customers [**51**].

Google's Personalized Search

Google keeps track of your search queries and the Web pages you have clicked. When you type in a new query, it can use this information to infer what you are interested in and return pages more likely to be what you are seeking. For example, the word "bass" has multiple meanings, but if you have a history of queries and page clicks related to fishing, but not music, that can help the search engine return the most appropriate pages.

Google is able to personalize search results whether or not you have a Google account. If you are signed in to Google, the search engine examines your Web history to personalize the search results. This information is held indefinitely, unless you delete your Web history. If you are not signed in, Google creates a cookie linked to your computer's browser, and it stores records of all queries associated with that cookie, as well as results that have been clicked, for up to 180 days [52].

Sidebar: Google Privacy Checkup

If you would like to limit the amount of information Google saves about your activities, Google offers a Privacy Checkup that lets you review and adjust your privacy settings. You can use Privacy Checkup to pause Google's collection of personal information in the following categories [53]:

- Web and App Activity: Your search queries and other Google activity
- Location History: Locations you have visited with signed-in devices, how often you have visited them, how long you have stayed, and common routes of travel
- Device Information: Your contact and calendar information, as well as information from apps and other devices
- Voice and Audio Activity: Recordings of your voice and accompanying audio
- YouTube Search History: Your YouTube search queries
- YouTube Watch History: A list of the YouTube videos you have watched

Collaborative Filtering

Collaborative filtering algorithms draw upon information about the preferences of a large number of people to predict

what an individual may enjoy. An organization performing collaborative filtering may determine people's preferences explicitly, through rankings, or implicitly, by tracking their purchases. The filtering algorithm looks for patterns in the data. Perhaps many people who purchase peanut butter also purchase jam. If a new customer buys a jar of peanut butter, the software may instruct the register to print out a discount coupon for a particular brand of jam along with the sales receipt. Collaborative filtering software is also used by online retailers and movie sites to make recommendations [54].

5.4.2 Opt-In Versus Opt-Out Policies

We have just examined a few ways in which a company that collects information about its customers' activities can use this information to provide its customers with a more personalized service. It only makes sense that if several companies pooled the information they had on the same person, they could construct a more complete electronic profile that would facilitate new insights into products or services that person might wish to purchase. What rules should govern the sharing of information collected by

organizations selling products or services? Two fundamentally different policies are called opt-in and opt-out.

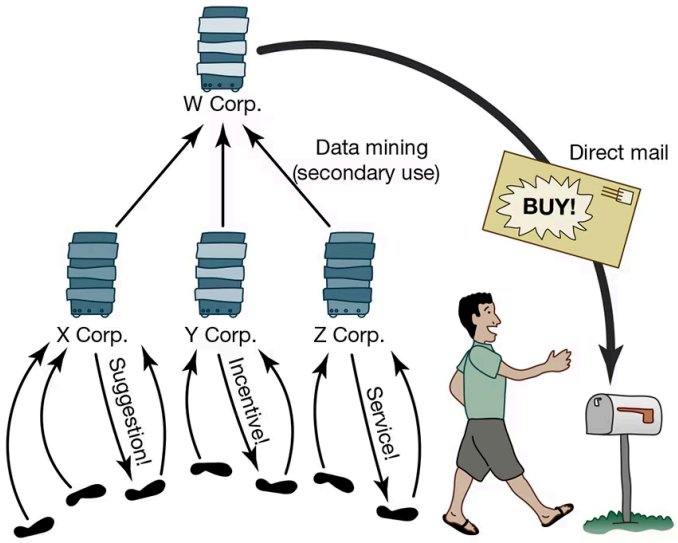
The **opt-in** policy requires the consumer to explicitly give permission for the organization to share the information with another organization. Opt-in policies are preferred by privacy advocates.

The **opt-out** policy requires the consumer to explicitly forbid an organization from sharing information with other organizations. Direct marketing associations prefer the opt-out policy because opt-in is a barrier for new businesses. New businesses do not have the resources to go out and collect all the information they need to target their mailings to the correct individuals. In an opt-out environment, most people will not go through the effort required to actually remove themselves from mailing lists. Hence it is easier for new businesses to get access to the mailing lists they need to succeed [55]. Another argument for opt-out is that companies have the right to control information about the transactions they have made. Information is a valuable commodity. An opt-in policy takes this commodity away from companies.

At this time opt-out policies are far more common than opt-in policies. Information about customers has *itself* become a commodity. Organizations sell or exchange information with

other organizations (Figure 5.4). This is a common way for organizations to gather large databases of information they can mine.

Figure 5.4



Companies use computers to record information about their customers and their buying habits. They analyze this information to suggest additional purchases, provide incentives, and deliver better service. They may also sell this information to other companies. By combining information from various sources, a company can build sophisticated profiles of individuals and target its direct-mail advertising to those people most likely to be interested in its products.

For example, a company selling time-share condominiums purchases from a hotel chain the names and addresses of people who have vacationed in a resort area in the past two years. From another organization it purchases a database that gives the approximate annual household income of a family, based on that family's nine-digit ZIP code. Combining these lists allows the time-share agency to target people most likely to have both the interest and the financial resources to

purchase a share of a vacation condominium. It uses direct mail to send brochures to these people.

Data mining can be surprisingly powerful. Suppose a government agency managing tollbooths were to sell information records of the following form:

⟨transponder number⟩ ⟨date⟩ ⟨time⟩ ⟨location⟩ ⟨charge⟩

The agency does not reveal the names of the owners of the cars, so it believes it is protecting their anonymity. However, many people have an account set up so that their tollbooth payments are automatically charged to their credit cards. If a credit card company buys these records from the tollbooth agency, it can match the date, time, and amount of the tollbooth payments with the date, time, and charge on its credit cards to determine the identity of the person driving a vehicle with a particular transponder number. Once this has been done, the credit card company can figure out which customers are driving the most miles and are likely to purchase new cars more frequently. It can then sell this information to banks interested in soliciting automobile loan applications [**29**].

5.4.3 Examples of Data Mining

Data mining is put to a wide variety of uses in modern society. Here are a few examples.

Targeting Pregnant Customers

The power of data mining was demonstrated in Target's efforts to identify which of its customers were pregnant. Retailers know that the habits of shoppers—where they buy certain goods and the brands they select—are difficult to change. However, when people graduate from college or move to a new town or get married, their shopping habits are more malleable. New parents are particularly open to changes in their shopping habits. For that reason Target asked its statisticians to find ways to predict which of Target's customers were in their second trimester of pregnancy. The company's goal was to use direct-mail offers to get them into the habit of buying a wide variety of items at Target stores.

Target's statisticians found customers who had set up baby-shower registries at Target, then looked back in time to discover what products they had bought when they were in

their second trimester. The analysts found about two dozen products that were good predictors of a second-trimester pregnancy, including unscented lotion, extra-large bags of cotton balls, and nutritional supplements. For those customers who were predicted to be pregnant, the statisticians showed they could also predict their expected delivery date within a relatively small window of time.

Target used the algorithms developed by its statisticians to mine its extensive databases of customer purchases. The company identified tens of thousands of customers who were probably pregnant and sent them direct-mail advertising. The marketing executives were savvy enough to know that the customers receiving these promotions might be upset if they discovered Target knew they were pregnant. In order not to tip them off, Target made sure that the mailings included offers on wineglasses, lawn mowers, and other unrelated items mixed in with the offers for diapers, baby clothes, and cribs [56].

Credit Reports

Credit reports are a great example of how information about customers has itself become a commodity. A credit bureau is a company that keeps track of an individual's assets, debts, and history of paying bills and repaying loans, using this

information to determine the creditworthiness of that person. Credit bureaus sell credit reports to banks, credit card companies, and other potential lenders.

Thanks to the national credit bureau system, you can get a credit card from a bank or store that you've never done business with. When you want to borrow money to purchase a home, you don't have to go to your local bank. You can get the money from a bank across the country that trusts you to repay the loan because of your high credit score. Competition among banks leads to lower interest rates, a definite advantage for consumers.

Of course, if you have a poor record of paying bills on time and repaying loans, your credit score will be low. People with low credit scores have a harder time getting loans and pay higher interest rates on the loans they do get.

A poor credit report can come back to haunt people in ways they might not have anticipated. Many employers conduct a credit check late in the job interview process as a way of double-checking a candidate before making a job offer. A credit report received by an employer doesn't give the applicant's credit score, but it does list the applicant's debts. Critics of the use of credit reports when making hiring decisions have stated that these reports can cause employers

to shy away from people of color and those who are currently out of work. “I think the assumption that is made is, if somebody is behind on their bills, then it tells something about their integrity or responsibility, but in many cases that assumption is flawed,” said Sarah Crawford of the Lawyers’ Committee for Civil Rights Under Law [57].

Targeted Direct Mail and Data Brokers

Years ago direct-mail marketing meant mass mailings of advertisements. Today the trend is toward targeted direct mail, in which businesses mail their advertisements only to the leads most likely to be interested in purchasing their products. Customized mailing lists are available from **data brokers**: companies that combine information gathered online with offline information, such as magazine subscriptions, loyalty cards, and government records, to create comprehensive profiles of consumers [58].

Edith Ramirez, then head of the US Federal Trade Commission, wrote: “You may not know them, but data brokers know you. They know where you live, what you buy, your income, your ethnicity, how old your kids are, your health conditions, and your interests and hobbies” [59].

Have you ever had a store clerk ask you for your ZIP code after you've made a purchase? It turns out that the clerk doesn't need your address to identify you. Your name (taken from your credit or debit card), combined with your ZIP code, is 90 percent accurate at identifying you and allowing your purchase to become another piece of information for data brokers [**60**].

Two of the most prominent data brokers are Experian (one of the three largest credit report companies in the United States) and Acxiom. Experian has a database of more than 200 million consumers. Acxiom is even larger. It has collected information on 500 million consumers, with an average of 1,500 pieces of information per consumer [**60**]. Both of these data brokers can provide specialized lists to direct marketers. For example, Acxiom has divided US households into 70 segments based on their demographics and their spending habits. These segments include one for affluent baby boomers, another for young singles, and another one for retirees of modest means.

Besides Experian and Acxiom, there are thousands of other data brokers, and many of them have created highly focused lists. For example, it is possible to purchase mailing lists of

people based on their sexual orientation, health status, or prior purchases [**61**].

Did you know that two shoppers visiting the same online retailer may have quite different experiences? Data brokers sell profiles of consumers to some online merchants, who use this information to determine which advertisements to display [**59**]. Retailers even use customer profiles to determine who should be offered a discount and who should be charged full price and offered more expensive options [**62**].

When Blue Chip Marketing Worldwide needed to identify candidates for an obesity drug trial, it looked for evidence that a person might be over their healthy weight, including a pattern of shopping for clothes online, frequent fast-food dining, and subscribing to premium cable TV packages [**63**]. Privacy experts warn that the success of these efforts demonstrates that the amount of data being collected has reached a point where companies can make accurate inferences about the medical conditions of individuals, even without accessing their private medical records.

Microtargeting

Since 2004 direct marketing based on data mining has become part of US presidential campaigns [**64**]. In a technique called **microtargeting**, a campaign combines data about voter registration, voting frequency, and contributions with consumer data and information available from a geographic information system to gain insights into which candidate the voter is likely to favor. The campaign then uses direct mailings, email, text messages, or home visits to encourage likely supporters to vote.

5.4.4 Social Network Analysis

A relatively new area in data mining is the incorporation of information collected from social networks. Here are a few examples of how organizations are using social network analysis to further their objectives.

)

Companies can track mentions of their brands on social media in real time. Social media sentiment analysis, or **opinion mining**, goes beyond simply counting mentions to analyze whether the comments are positive or negative. Companies track sentiment in real time and can be alerted

when sentiment suddenly changes, allowing them to respond quickly to negative mentions [**65**].

About two in five employers in the United States include analysis of social network sites in their background checks of job candidates, and half of these employers report they have found information that has caused them not to hire certain candidates. The most common reasons for rejecting candidates were the discovery of posts containing sexually provocative or inappropriate photos, information about drinking or drug use, criticisms of former employers or coworkers, evidence of poor communication skills, and discriminatory remarks about other people. Interestingly, one-quarter of employers conducting social media background checks reported they had also discovered positive information about a job candidate that led to an immediate job offer [**66**].

Banks are combining data collected from social networks with credit card statements and other information to evaluate the riskiness of loans. For example, someone applying for a loan to start a new business may be a bad risk if the proposed business has no connection with their social network, educational background, travel history, or previous business dealings [**67**].

In ultracompetitive cell phone markets, it's crucial that companies keep their subscribers from defecting to rival firms. Bharti Airtel, India's largest cell phone company, uses software to analyze phone records and identify "influencers," those subscribers most likely to be able to persuade their friends and family members to follow them when they switch carriers. It then offers the influencers special promotions to keep them loyal. How can Bharti Airtel identify influencers from their phone records? They are the ones whose calls are quickly returned, who call other people late at night more frequently, and who get more calls on Friday afternoons when parties are often organized [**67**].

Speaking of parties, police in Richmond, Virginia, monitor Facebook and Twitter messages to determine where parties are happening. Data-mining software identifies the party locations mentioned most frequently. By deploying officers more strategically on big party nights, the department saves about $15,000 on overtime pay, and the community has seen a big drop in criminal activity [**67**].

Sidebar: Controlling Your Facebook Information

If you're worried about what others can learn about you through postings on Facebook, but don't want to delete your Facebook account, you can change your settings to minimize who can see what you're doing. The following list shows the ways in which you can restrict the flow of personal information. You may decide to have more privacy in some areas and less privacy in other areas. Use Facebook's "Privacy Checkup" feature to view and change your settings. The names of all these settings are quoted verbatim from the Facebook Web site [68].

Under "Profile Information," you can restrict who sees the following information about you:

- Phone number
- Email
- Birthday
- Hometown
- Relationship

- Current city
- Education
- Who can see your friends list on your profile
- Who can see the people, pages and lists you follow

Under “Posts and Stories,” you can restrict who sees your posts and stories:

- Who can see your future posts
- Who can see your stories
- Limit past posts to only Friends

Under “Blocking,” you can create a list of people who will no longer be able to view your posts, tag you, send you invitations, “start a conversation” with you, or “add you as a friend.”

5.4.5 Release of “Anonymized” Datasets

On at least two occasions, corporations have released large datasets from which they had attempted to strip away personally identifiable information in order to preserve the anonymity of the people creating the data. In neither case were the datasets truly anonymized.

Netflix Prize

Netflix is a popular subscription service for movies and television shows. An important feature of Netflix is its movie recommendation service. After a subscriber has rated several movies, Netflix uses a collaborative filtering algorithm to predict how well the subscriber will like other movies in its collection. It then recommends to the subscriber movies the subscriber is likely to enjoy.

In 2006 Netflix offered a $1 million prize to any group that could come up with a collaborative filtering algorithm that was at least 10 percent better than Netflix's own algorithm at predicting user ratings for movies. Netflix released more than 100 million movie ratings from nearly half a million customers, stripped of private information in an attempt to make the records anonymous. Each movie rating consisted of four pieces of information—subscriber, movie, date of grade,

and grade—where each subscriber was represented by an integer.

However, a group of researchers at the University of Texas at Austin demonstrated how it was possible, with just a little information about movies seen by an individual, to identify the movie-rating records associated with that person, revealing potentially sensitive information, such as their political leanings or sexual orientation [**69**]. The revelation that the release of "anonymous" movie ratings information could compromise the privacy of Netflix subscribers led to a complaint by the US Federal Trade Commission and a lawsuit. On March 12, 2010, Netflix announced that it was canceling a Netflix Prize sequel [**70**].

AOL Search Dataset

In 2006 an AOL research team led by Dr. Abdur Chowdhury posted to the Web a file containing three months' worth of search queries from about 650,000 AOL users. The purpose of releasing the information was to support university research, but the dataset was downloadable by anybody with a Web browser and a fast enough Internet connection [**71**].

In an attempt to anonymize the dataset, which consisted of about 20 million queries, the AOL team used a random

integer identifier, rather than a name or other personal identifier, to label all the queries submitted by the same user [71]. However, researchers who studied the dataset determined almost immediately that examining a set of queries with the same integer identifier often provided enough information to identify the user. For example, many people apparently performed searches on their names, presumably to see which Web links were returned. Addresses and social security numbers also appeared in queries [72]. Within days, reporters from the *New York Times* identified several of the people whose search results had been posted. Thelma Arnold from Liburn, Georgia, agreed to be identified by the newspaper as user #4417749 [73].

Responding to a storm of negative publicity, AOL took down the dataset three days after posting it, but by then it was too late: copies had already been downloaded and reposted on other Web sites [72]. As the public outcry continued, AOL fired Dr. Chowdhury and his supervisor. Maureen Govern, the chief technology officer of AOL, resigned [71].

According to Kurt Opsahl of the Electronic Frontier Foundation, AOL made two mistakes. The first mistake was failing to get the consent of AOL users before making their queries available to third parties. The second mistake was

posting the dataset to the Web, rather than making it available only to university researchers who had agreed to follow reasonable privacy protections [74].

Large Language Models

Modern chatbots like ChatGPT are powered by large language models, which are trained on data scraped from the Internet. In 2021 a group of researchers revealed that it is possible to perform a "training data extraction attack" on large language models, causing them to reveal individual training examples that may contain sensitive data. The researchers chose GPT-2 to demonstrate their point because the model and the training data had already been made public. Their attack on GPT-2 revealed hundreds of training examples containing names, phone numbers, physical addresses, and email addresses. The researchers concluded that large language models are more vulnerable to training data extraction attacks than smaller language models [75].

5.5 Examples of Consumer or Political Backlash

Advances in information technology have led to a drop in the cost of acquiring information. Meanwhile, the value of information continues to rise, as organizations refine their data-mining techniques. The result of these trends is that corporations have an incentive to acquire more information, making it more difficult for individuals to protect their privacy [21]. Still, people and their representatives can and do fight back when they feel a corporation has gone too far.

5.5.1 Marketplace: Households

Lotus Development Corporation teamed up with credit reporting company Equifax to develop a database on 120 million people and a program in CD format that would allow the user to produce direct-mailing lists based on various criteria, such as household income. Lotus hoped to sell the

package, which it called “Marketplace: Households,” to small businesses. Soon after the product was announced in the spring of 1990, there was a considerable backlash. Consumers complained loudly and vigorously, with more than 30,000 letters, phone calls, and emails. Lotus dropped plans to sell the CD [76].

How times have changed! A little more than two decades later, data brokers Acxiom and Experian are selling direct-mailing lists based on much more detailed information about consumers (as you read in the discussion of targeted direct mail in Section 5.4.3).

5.5.2 Facebook Beacon

In November 2007, Facebook announced Beacon, “a core element of the Facebook Ads system for connecting businesses with users and targeting advertising to the audiences they want” [77]. Beacon promised to be an important way for Facebook to earn advertising revenue. Fandango, eBay, and 42 other online businesses paid Facebook to do “word-of-mouth” advertising of their products and services through Beacon. For example, after a Facebook user bought movie tickets on Fandango, Fandango

would send this information to Facebook so that Facebook could broadcast it to that user's friends.

Beacon was based on an opt-out policy, meaning that it was in effect unless a user explicitly asked to be excluded. That decision was good for Facebook because advertising revenue depends on the size of the audience. However, the decision to make the system opt-out upset many Facebook users, who were unaware of Beacon until it revealed information they thought was private. For example, after Sean Lane purchased what was supposed to be a surprise Christmas gift, the following news headline was broadcast to his wife and more than 700 other people in his Facebook network: "Sean Lane bought 14K White Gold 1/5 ct Diamond Eternity Flower Ring from overstock.com" [78].

Beacon soon attracted strong criticism from a variety of sources. A spokesperson for MoveOn.org said, "Sites like Facebook are revolutionizing how we communicate with one another and organize around issues together in a 21st century democracy. The question is: Will corporate advertisers get to write the rules of the Internet or will these new social networks protect our basic rights, like privacy?" [78]. MoveOn.org created an online group calling for Beacon to require an explicit opt-in from users, and it attracted the

support of more than 50,000 Facebook users. A few weeks later, Facebook decided to switch to an opt-in policy for Beacon. “I’m not proud of the way we’ve handled this situation, and I know we can do better,” said Mark Zuckerberg, CEO of Facebook [79].

5.5.3 Malls Track Shoppers’ Cell Phones

On Black Friday, 2011, two malls in the United States—the Promenade Temecula in California and the Short Pump Town Center in Virginia—began recording the movement of shoppers through the stores by tracking the locations of their cell phones. The malls hoped to be able to answer such questions as these:

- How much time do people spend in store X?
- How many people who shop at store Y also shop at store Z?
- Are there unpopular areas of the mall that do not attract enough shoppers?

Small signs posted throughout the malls informed shoppers of the study. It let them know that the data were being

collected anonymously; the mall assigned an ID code to each phone and tracked the movements of the phone without knowing anything about the person carrying the phone. To prevent data about their movements from being collected, shoppers had to turn off their cell phones.

The malls had planned to continue their study through the Christmas buying season, but an intervention by Senator Charles Schumer of New York prompted them to stop collecting data after only three days [80].

Sharon Biggar, CEO of Path Intelligence, the British firm that made the cell phone tracking equipment, responded to the senator's statements by pointing out that online retailers track far more information about their customers' shopping habits without asking them for permission. "We are simply seeking to create a level playing field for offline retailers," she said [80].

5.5.4 iPhone Apps Uploading Address Books

In February 2012, programmer Arun Thampi in Singapore discovered that the app for the social networking site Path was uploading his iPhone's address book without first getting

his permission. Thampi wrote on his blog, “I’m not insinuating that Path is doing something nefarious with my address book but I feel quite violated that my address book is being held remotely on a third-party service” [81].

David Morin, the CEO of Path, initially replied to Thampi’s post by saying that the purpose of collecting the information was to make it easier for people to connect with family and friends on Path and to let them know when people in their address book join Path. Morin’s statement also labeled Path’s actions as an “industry best practice.” However, it didn’t take long for the Internet community to weigh in and point out that Apple’s guidelines require apps to ask for permission before uploading information from address books. Facing a storm of negative publicity, Morin issued another statement in which he apologized for what Path had done, promised that the company would destroy the data it had collected, and announced that the app would be changed so that it would no longer upload address books without permission [82].

As the Path controversy erupted, the media pointed out that other popular iPhone apps, including Twitter, Foursquare, and Instagram, were also gathering information from address books without asking for permission. All the aforementioned

companies responded by announcing that they, too, would release new versions of their apps that explicitly asked users for permission before uploading contact information from address books [83]. Apple took the additional step of introducing an App Tracking Transparency function, which gives iPhone users the ability to control which apps can access their data.

5.5.5 Instagram's Proposed Change to Terms of Service

In December 2012, the popular photo-sharing service Instagram announced an upcoming change in its privacy policy and terms-of-service agreement. The terms-of-service agreement appeared to change how Instagram and its parent company, Facebook, could use photographs uploaded by Instagram users. The proposed agreement included the following statement:

> **You agree that a business or other entity may pay us to display your username, likeness, photos (along with any associated metadata), and/or actions you take, in connection with paid or**

> **sponsored content or promotions, without any compensation to you. [84]**

After some legal experts said that the new terms-of-service agreement would allow Instagram or Facebook to use photos on the Instagram site in advertisements without compensating or even getting the permission of the person who uploaded them, the reaction was swift. The hashtag #Boycottinstagram began trending on Twitter, and many Instagram users downloaded alternative photo-sharing apps. The number of people using Pheed and Flickr increased significantly, though the total number of users of these services remained far below the 100-plus million using Instagram [85].

Responding to the uproar, Instagram co-founder Kevin Systrom issued a statement saying that the new privacy policy and terms of service had been misunderstood. He also announced that the advertising section in the terms-of-service agreement was being changed back to its original version [86].

5.5.6 The *Daily Telegraph*

The *Daily Telegraph* newspaper in London installed heat and motion sensors at employees' desks in 2016. The newspaper had planned to use the information it collected to reduce power consumption for lighting, heating, and cooling during periods of low building occupancy. However, employees feared the devices would be used for surveillance, and when they complained through their union, the newspaper removed the sensors [87].

5.5.7 Cambridge Analytica

Billionaire computer scientist Robert Mercer envisioned creating a sophisticated data analytics firm that would allow him to play an important role in the political success of conservative candidates and causes. He was intrigued by work being done by the elections division of SCL Group, a British firm, to develop "psychographic profiles" of adults that would classify their personalities and predict their political preferences [88]. In 2014 Mercer invested $15 million in a joint venture with SCL Group, forming a shell corporation called Cambridge Analytica in the United States. The CEO of Cambridge Analytica, Alexander Nix, was also an employee of SCL Group, and all of the contracts signed by

Cambridge Analytica were actually serviced by SCL Group [89].

In order to win business from US political campaigns, Cambridge Analytica had to create psychographic profiles of millions of American voters. SCL Group contacted Cambridge University's Psychometrics Centre, where researchers had been experimenting with creating psychological profiles of people based on what content they had liked on Facebook. After the Psychometrics Centre refused to work with SCL Group, the firm struck a deal with Aleksandr Kogan, a lecturer at Cambridge University who was familiar with psychometrics [89].

Aleksandr Kogan and Joseph Chancellor co-founded Global Science Research [90]. They created a survey app called "thisisyourdigitallife" and used Amazon's Mechanical Turk to attract people to the survey. Global Science Research offered $1 or $2 to take a personality test, on two conditions. First, the company was only interested in Americans. Second, the test-takers had to access "thisisyourdigitallife" using Facebook Login. The app's terms and conditions pop-up revealed that the app would "download some information about you and your network. . . basic demographics and likes

of categories, places, famous people, etc. from you and your friends" [**91**].

About 270,000 people took the survey, giving Global Science Research access to data from their personal profiles. The company was also able to access the personal data of as many as 87 million people—mostly Americans—who were on the friends lists of the survey takers and who had not adjusted their privacy settings to prevent such a disclosure [**92**, **93**]. (This sort of information gathering from Facebook friends is no longer possible. On April 30, 2015, Facebook changed its software interface, making it impossible for an app to mine data from the friends of the app's users [**94**].)

Global Science Research shared the profiles with Cambridge Analytica. About 30 million of these profiles had enough identifying information, such as addresses, that Cambridge Analytica could combine the data with other data they had access to and construct psychographic profiles [**89**]. The company classified voters over five personality traits: openness, conscientiousness, extroversion, agreeableness, and neuroticism. For example, Cambridge Analytica held that voters classified as neurotic were more likely to be influenced by "rational and fear-based" arguments, while voters classified as introverted should be sent messages that

reference “tradition and habits and family and community” [**91**].

The 2016 campaign of US presidential candidate Ted Cruz hired Cambridge Analytica and began microtargeting voters based on the data acquired from Facebook users [**95**]. The value of the data Cambridge Analytica provided to the Cruz campaign is debatable. Members of the Cruz campaign told the *New York Times* that in the Oklahoma primary election campaign, more than half of the names of supposed Cruz supporters they had been given by Cambridge Analytica turned out to favor other Republican candidates [**88**].

When Ted Cruz’s campaign faltered, Cambridge Analytica began working for the campaign of Donald Trump, which paid the firm $5 million in September 2016 alone. The firm claimed to know how to identify millions of voters most likely to vote for Trump [**96**].

When the story about Cambridge Analytica broke in 2018, Facebook responded by stating that it was not a data breach, noting that everyone who used Aleksandr Kogan’s app had granted their consent for him to access their information, and the privacy settings of users’ friends also allowed their information to be shared [**93**]. Instead, Facebook said Kogan was to blame, claiming that he had scammed them and

perpetrated a fraud by sharing with Cambridge Analytica information that was supposedly gathered for academic research purposes. Facebook suspended the accounts of Kogan and Cambridge Analytica in March 2018 [89]. Curiously, Facebook had hired Joseph Chancellor, who co-founded Global Science Research with Kogan, in November 2015. Chancellor was still working for Facebook in March 2018 [90].

Politicians joined the public outcry resulting from the disclosure that Cambridge Analytica had acquired information about tens of millions of Americans without their permission. Mark Zuckerberg, the CEO of Facebook, was called to Washington, DC, to testify for a total of 10 hours in front of 91 lawmakers on two Congressional committees [97]. In May 2018 Cambridge Analytica announced it was ceasing most operations and filing for bankruptcy [98].

Summary

This chapter has focused on privacy issues brought to the forefront by the introduction of modern information technology. The issues of privacy and intellectual property are similar in the sense that both issues relate to how information ought to be controlled. Modern information technology makes it much easier to collect and transmit information, whether it be a song, a Social Security number, or a shopping list. Privacy can be seen as a balancing act among the desires of the individual, the profit motive of companies, and the common good. The individual seeks to restrict access to personal information. Companies seek to gather information and sell it to those who want access to it. The common good dictates that some information should be widely known. Society must decide which information ought to be private, which information can be gathered and sold, and which information should be public.

Communities require that some information be knowable to all. A public record is a piece of information collected by a government agency. Certain events, such as a home purchase,

the birth of a child, and a criminal conviction, result in the creation of a public record.

Often we voluntarily share information with others in order to get something else we want. For example, there is a tension between privacy and trust. We desire privacy, but we also want others to trust us. In some situations we must reveal some personal information in order to win the trust of others. For example, in order to obtain a mortgage loan, applicants must provide lenders with proof of their income by turning over pay stubs and income-tax statements.

We participate in many activities in which private organizations collect information about us. Data mining is a way for organizations to create a complex profile of a person from a large collection of individual facts. Companies use data mining to direct advertising to the most promising customers. Data mining is possible because organizations handling transactions have the right to sell information about these transactions to other organizations. Whether to provide customers with better service, increase their revenues, or both, companies frequently push the boundaries of what consumers are willing to tolerate.

Further Reading, Listening, and Viewing

Elizabeth Alex and Mark Clegg. “Smartphone Pictures Pose Privacy Risks.” *KSHB/NBC Action News*, November 9, 2010. 3:56. www.youtube.com/watch?v=N2vARzvWxwY.

Robby Bryant and Bryan Horling. “Personalized Search.” Google, December 4, 2009. 1:32. www.youtube.com/watch?v=EKuG2M6R4VM.

Charles Duhigg. “How Companies Learn Your Secrets.” *New York Times Magazine*, February 16, 2012.

Jo Ling Kent. “Lawsuit: Zillow ‘Zestimates’ Are Wrong, Preventing Homes from Selling.” *NBC News*, May 26, 2017. 1:39. www.youtube.com/watch?v=19BfEEtpcgg.

Thorin Klosowski. “Your Phone’s Location Access Reveals a Lot. Here’s How to Turn It Off.” *New York Times*, June 29, 2022. https://www.nytimes.com/wirecutter/blog/turning-off-phone-location-access/.

Steve Kroft. “The Data Brokers: Selling Your Personal Information.” *60 Minutes*, March 9, 2014. 14:22. www.cbs.news.com.

Steven Levy. “How Early Twitter Decisions Led to Anthony Weiner’s Dickish Demise.” *Wired Epicenter*, June 13, 2011. www.wired.com/epicenter/.

Evan Ratliff. “Writer Evan Ratliff Tried to Vanish: Here’s What Happened.” *Wired*, November 20, 2009. www.wired.com/2009/11/ff_vanish2/.

Jeffrey Rosen. “The Web Means the End of Forgetting.” *New York Times*, July 21, 2010. www.nytimes.com.

Elizabeth Schulze. “GDPR: Why Everyone Is Freaking Out Over Four Letters.” *CNBC*, June 14, 2018. 2:53. www.cnbc.com/2018/03/30/gdpr-everything-you-need-to-know.html.

Christopher Wylie. Interview by Carole Cadwalladr. “Cambridge Analytica Whistleblower: ‘We Spent $1 Million Harvesting Millions of Facebook Profiles.’” *Guardian*, March 26, 2018. 13:03. www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far.

"Data Mining vs. Data Privacy." *Deutsche Welle*. Accessed June 24, 2018. 4:05. www.dw.com/en/data-mining-vs-data-privacy/av-43493760.

Review Questions

1. What is the difference between having privacy and being alone? Provide examples.
2. How can an excess of privacy cause harm? How can a lack of privacy cause harm?
3. What does it mean to say privacy is a prudential right?
4. Is privacy a negative right or a positive right?
5. Why is it important that some information be made available to everyone through public records?
6. Provide an example (not already given in the book) of a situation where people must disclose personal information to a private organization in order to obtain a product or service.
7. How do retailers use loyalty cards to improve their sales?
8. What are the advantages of consolidating a patient's medical records into a single database accessible by

many? What are the risks associated with this consolidation?

9. How could “cookies” created by a Web server affect a computer user’s privacy?

10. What is the difference between data mining and collaborative filtering?

11. Explain the difference between an opt-in policy and an opt-out policy. Which policy is favored by privacy advocates?

12. What lesson should we draw from the release of large datasets in which personal identifiers were replaced by integers?

Discussion Questions

13. Do you agree with Scott McNealy's statement that people have "zero privacy" and should just get over it?

14. If people value privacy so much, why do they put so much personal information on their Facebook pages and in their blogs?

15. MIT computer science professor Harold Abelson has said, "In today's online world, what your mother told you is true, only more so: people really can judge you by your friends" [99]. Have you ever been upset or embarrassed by what your friends posted on Facebook? Are you concerned that people are going to judge you based on what your friends are posting?

16. Should mobile apps be allowed to collect information about your location and transmit this information to data brokers?

17. Warren and Brandeis argued that it is a violation of a person's privacy to take their photograph without their consent.

    a. Do you agree with their position? Why or why not?

    b. If someone takes your photo, should you just assume it's going to be posted on the Web?

18. What is the difference between privacy and anonymity?

19. Do you agree with the author that it is more difficult to know whom to trust in modern society than it was in a small village of a few centuries ago? Why or why not?

20. Critics of grocery club cards give examples of card-member prices being equal to the regular product price at stores without customer loyalty programs. In other words, customers who want to get food at the regular price must use the card. Customers pay extra if they don't want to use the card. Is it fair for a store to charge us more if we don't want to use its loyalty card? Explain your reasoning.

21. Some consumers give phony personal information when they apply for rewards or loyalty cards at stores. Others take it a step further by regularly exchanging

their cards with those held by other people. Are these people doing anything wrong? Why or why not?

22. If you voluntarily have your body scanned at a department store, who should own that information, you or the store? Should the store have the right to sell your body measurements to other businesses? Explain your reasoning.

23. TiVo keeps detailed information about the television-viewing habits of customers who subscribe to its service.

    a. Should your television-viewing habits be private information?

    b. Do you care if anyone else knows what television shows or movies you have watched in the past year?

    c. Do voters have the right to know the viewing habits of people running for elected office?

24. Enhanced 911 service allows cell phone companies to track the locations of active cell phone users within 100 meters.

    a. Who should have access to location information collected by cell phone companies?

b. How long should this information be kept?

c. If this information could be used to help you establish an alibi, would you want the cell phone company to be able to release it to the police?

d. How would you feel about the cell phone company releasing compromising information about your whereabouts to the police?

e. Should the police be able to get from the cell phone company the names of all subscribers using their phones close to a crime scene around the time of the crime?

25. Should parents implant microchips in their children to make them easier to identify in case they are lost or kidnapped? Why or why not?

26. Before offering a job candidate a position, some potential employers do a criminal background check of the candidate. What are the pros and cons of this policy?

27. You are setting up an account at a local store that rents outdoor equipment (tents, backpacks, ski gear, etc.). The clerk asks you to fill out the application form completely. One of the fields asks for your Social

Security number. You leave that field blank. The clerk refuses to accept your application without the field filled in. You ask to speak to the manager, and the clerk says the manager is not available. Would it be wrong in this situation to fill in a fake Social Security number?

28. A company discovers that some of its proprietary information has been revealed in Internet chat rooms. The disclosure of this information results in a substantial drop in the price of the company's shares. The company provides Internet service providers with the screen names of the people who posted the confidential information. It asks the ISPs to disclose the actual identities of these people. Should the ISPs comply with this request? Explain your reasoning. (This scenario is adapted from an actual event [100].)

29. Google Glass (no longer sold) provided an information display in eyeglass frames, making it easier for people to view information while on the go. Instead of having to look at the screen of a tablet or smartphone, Google Glass users could see text and images displayed in their field of vision. Google Glass also contained a camera and a microphone, enabling users to take photos and shoot videos from a first-person perspective. Do you

believe Google Glass represented a significant new threat to privacy? Under what circumstances, if any, is it inappropriate for someone to wear a product like Google Glass?

30. Homer Gaines used Google Glass while making a marriage proposal to his girlfriend, Tami Stillwell. "I would not have been able to pull off that level of spontaneity with any other device and instantly share it with the world. Glass gave me the ability to share with everyone that special moment from my point of view—the surprise on her face, the way she jumped around, the ring on her finger and the tears of joy in her eyes" [**101**]. What are your reactions to this episode?

31. What special responsibilities do computer professionals have with respect to understanding and protecting the privacy rights of their fellow citizens?

In-Class Exercises

32. Give an example of a piece of information that a person should not have to reveal to anyone else. Give an example of a piece of information that society should be able to demand that a person reveal.

33. Divide the class into groups, with about four persons in every group. Half the groups should come up with evidence supporting the proposition "We live in a global village." The remaining groups should come up with evidence supporting the proposition "We live in a world of strangers." After a suitable period of time, the groups should share their findings.

34. When you purchase a product or service using a credit card, the merchant has information linking you to the transaction. Divide the class into two groups (pro and con) to debate the proposition that merchants should be required to follow an opt-in policy. Such a policy would require the consumer to explicitly give permission before a merchant could share information about that consumer with another organization.

35. Joe Herzenberg was a historian and politician as well as the first openly gay elected official in North Carolina. After he died in 2007, his papers, including correspondence, photographs, diaries, and other materials, were donated to the Southern Historical Collection (SHC). Herzenberg kept a record of his personal and professional accomplishments and struggles in a series of diaries spanning more than 50 years. In the diaries, "Herzenberg documents his sexual encounters and alludes to his friends' sexual relationships and illegal activities" [**102**].

According to Laura Clark Brown, "Most SHC collections are unrestricted for both research and duplication in the SHC's search room. In that relatively controlled environment, [the SHC transfers] the responsibilities for the use of sensitive materials to the researcher" [**102**]. SHC librarians must decide whether they should digitize the contents of Joe Herzenberg's diaries and make them available on the Web. Debate the following proposition: The SHC librarians should not digitize the contents of Joe Herzenberg's diaries until everyone mentioned in the diaries has either given permission or died.

36. Research the case *Google Spain* v. AEPD *and Mario Costeja González*. This case pits a particular kind of privacy—the right for certain information not to show up in a search result—against the right to free expression.

    Divide the class into groups of four or five students. Each group should debate the following proposition: An individual should have the right to force a search engine to delete links to pages containing information that is correct but no longer relevant. After a reasonable length of time, groups should take turns sharing their conclusions with the rest of the class.

References

[1] Polly Sprenger. "Sun on Privacy: 'Get Over It.'" *Wired*, January 26, 1999. www.wired.com.

[2] Gary Horcher. "Woman Says Her Amazon Device Recorded Private Conversation, Sent It Out to Random Contact." *KIRO 7 News*, May 25, 2018. www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private- conversation-sent-it-out-to-random-contact/755507974.

[3] Edmund F. Byrne. "Privacy." In *Encyclopedia of Applied Ethics*, edited by Ruth F. Chadwick, volume 3, pp. 649–659, Academic Press, Waltham, MA, 1998.

[4] Edward J. Bloustein. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prossera." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, pp. 156–202, Cambridge University Press, Cambridge, England, 1984.

[5] Ferdinand Schoeman. "Privacy: Philosophical Dimensions of the Literature." In *Philosophical Dimensions of Privacy: An Anthology*, edited by

Ferdinand David Schoeman, pp. 1–33, Cambridge University Press, Cambridge, England, 1984.

[6] Edmund Ronald Leach. *A Runaway World?* British Broadcasting Corporation, London, England, 1967.

[7] Marie Hartwell-Walker. "Why Dysfunctional Families Stay That Way." *Amherst Bulletin*, January 28, 1994.

[8] Morton H. Levine. "Privacy in the Tradition of the Western World." In *Privacy: A Vanishing Value?*, edited by William C. Bier, SJ, pp. 3–21, Fordham University Press, New York, NY, 1980.

[9] Jeffrey H. Reiman. "Privacy, Intimacy, and Personhood." *Philosophy & Public Affairs,* 6(1):26–44, 1976. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, Cambridge University Press, Cambridge, England, 1984.

[10] Stanley I. Benn. "Privacy, Freedom, and Respect for Persons." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, pp. 223–244, Cambridge University Press, Cambridge, England, 1984.

[11] Charles J. Sykes. *The End of Privacy*. St. Martin's Press, New York, NY, 1999.

[12] Gini Graham Scott. *Mind Your Own Business: The Battle for Personal Privacy*. Insight Books/Plenum Press, New York, NY, 1995.

[13] Constance T. Fischer. "Privacy and Human Development." In *Privacy: A Vanishing Value?*, edited by William C. Bier, SJ, pp. 37–45, Fordham University Press, New York, NY, 1980.

[14] Robert C. Neville. "Various Meanings of Privacy: A Philosophical Analysis." In *Privacy: A Vanishing Value?*, edited by William C. Bier, SJ, pp. 22–33, Fordham University Press, New York, NY, 1980.

[15] Joseph G. Keegan, SJ. "Privacy and Spiritual Growth." In *Privacy: A Vanishing Value?*, edited by William C. Bier, SJ, pp. 67–87, Fordham University Press, New York, NY, 1980.

[16] Charles Fried. "Privacy: A Moral Analysis." *Yale Law Review*, 77:475–493, 1968. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, Cambridge University Press, Cambridge, England, 1984.

[17] James Rachels. “Why Privacy Is Important.” *Philosophy & Public Affairs,* 4(4):323–333, 1975. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, Cambridge University Press, Cambridge, England, 1984.

[18] Samuel D. Warren and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review,* 4(5): 193–220, December 15, 1890.

[19] William L. Prosser. “Privacy: A Legal Analysis.” *California Law Review,* 48:338–423, 1960. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, Cambridge University Press, Cambridge, England, 1984.

[20] Judith Jarvis Thomson. “The Right to Privacy.” *Philosophy & Public Affairs,* 4(4):295–314, 1975. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman, Cambridge University Press, Cambridge, England, 1984.

[21] Alexander Rosenberg. “Privacy as a Matter of Taste and Right.” In *The Right to Privacy*, edited by Ellen Frankel Paul, Fred D. Miller Jr., and Jeffrey Paul, pp.

68–90. Cambridge University Press, Cambridge, England, 2000.

[22] Steven L. Nock. *The Costs of Privacy: Surveillance and Reputation in America*. Aldine de Gruyter, New York, NY, 1993.

[23] Michael L. Sankey and Peter J. Weber, editors. *Public Records Online: The National Guide to Private & Government Online Sources of Public Records*. 4th ed. Facts on Demand Press, Tempe, AZ, 2003.

[24] Ben Popken. "New Service Adds Your Drunken Facebook Photos to Employer Background Checks, for Up to Seven Years." *Consumerist*, June 21, 2011. www.consumerist.com.

[25] Social Intelligence (Web site). Accessed October 15, 2013. www.socialintel.com.

[26] Justin Mitchell. "Making Photo Tagging Easier." *The Facebook Blog*, December 15, 2010. blog.facebook.com.

[27] "EPIC Complaint in Re: Facebook and the Facial Identification of Users." Federal Trade Commission, June 10, 2011.

[28] Rachel King. “Facebook Photo Tag Suggestions: What’s So Bad About Them Anyway?” *Between the Lines* (blog), June 9, 2011. www.zdnet.com.

[29] Jay Warrior, Eric McHenry, and Kenneth McGee. “They Know Where You Are.” *IEEE Spectrum*, 20–25, July 2003.

[30] Elizabeth Montalbano. “Microsoft Helps Put Ads on Computerized Shopping Carts.” *IDG News*, January 16, 2008. www.pcworld.com.

[31] John Vanderlippe. “Supermarket Cards: An Overview of the Pricing Issues.” Consumers Against Supermarket Privacy Invasion and Numbering, 2003. www.nocards.org/overview.

[32] Elizabeth Weise. “Identity Swapping Makes Privacy Relative.” *USA Today*, June 6, 2000.

[33] Stephanie Clifford. “Shopper Alert: Price May Drop for You Alone.” *New York Times*, August 10, 2012.

[34] Amy Tsao. “So, We’ll Take It In. . . .” *Retail Traffic*, May 1, 2003.

[35] Charles J. Murray. “Privacy Concerns Mount over Retail Use of RFID Technology.” *Electronic Engineering Times* (1298), December 1, 2003.

[36] Meg McGinty. “RFID: Is This Game of Tag Fair Play?” *Communications of the ACM*, 47(1):15–18, January 2004.

[37] “Owners of Dogs Lacking Implants Face Fines.” *China Post*, September 1, 2000.

[38] Amal Graafstra. “How Radio-Frequency Identification and I Got Personal.” *IEEE Spectrum*, March 2007.

[39] Duncan Graham-Rowe. “Clubbers Choose Chip Implants to Jump Queues.” *New Scientist*, May 21, 2004. www.newscientist.com.

[40] “Parents Look to Microchip Children.” CNN.com/World, September 3, 2002. archives.cnn.com.

[41] Lylah M. Alphonse. “In the Parenthood.” Boston.com Moms, June 9, 2010. www.boston.com.

[42] Andrew Leonard. “Angry Birds, Tracking Device?” *Salon* (Web site), January 18, 2013. www.salon.com.

[43] Kurt Wagner. “Here’s How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users.” *Recode* (Web site), March 17, 2018. www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

[44] Tom Krisher. "OnStar Halts Stolen SUV in Visalia Police Chase." BakersfieldNow.com, Bakersfield, California, October 19, 2009. www.bakersfieldnow.com.

[45] "OnStar Takes on Conspiracy Theorists." *Edmunds InsideLine*, November 13, 2009. www.insideline.com.

[46] Ian Austen. "Your Brake Pads May Have Something to Say (by E-mail)." NYtimes.com, March 27, 2003.

[47] Editorial. "Your E-Health Records." *New York Times*, January 31, 2009.

[48] American Civil Liberties Union. "Seizure of Rush Limbaugh's Medical Records Violates Florida's Constitutional Right of Privacy, ACLU Tells Court" (press release). February 17, 2004. www.aclu.org.

[49] "TiVo: Viewers Skip Fewer 'Relevant Ads.'" *Adweek*, July 30, 2008. www.adweek.com.

[50] Jeff Blake. "What's with All the Privacy Notices and Website Cookie Notification?" *Houston Press*, May 25, 2018.

[51] L. A. Lorek. "Data Mining Extracts Online Gold; Stores Collect Information About Web Customers to

Target Future Sales Pitches." *San Antonio Express-News*, December 15, 2002.

[52] "Personalized Search: Basics." Google Web site. Accessed September 2, 2011. www.google.com/support.

[53] "Decide Which Privacy Settings Are Right for You." Google (Web site), Accessed June 10, 2018. myaccount.google.com/privacy.

[54] "United We Find." *Economist*, March 10, 2005.

[55] Carolyn Hirschman. "Congress Sticks Its Nose into Online Privacy." *Telephony,* 241(7), August 13, 2001.

[56] Charles Duhigg. "How Companies Learn Your Secrets." *New York Times Magazine*, February 16, 2012.

[57] Katie Leslie and Marcus K. Gamer. "Poor Credit Prevents Some from Scoring a Job." *Chicago Tribune*, November 12, 2010. articles.chicagotribune.com.

[58] Craig Timberg. "Brokers Use 'Billions' of Data Points to Profile Americans." *Washington Post*, May 27, 2014. www.washingtonpost.com.

[59] Gary Anthes. "Data Brokers Are Watching You." *Communications of the ACM*, January 58(1): 28–30,

2015.

[60] Natasha Singer. “Mapping, and Sharing, the Consumer Genome.” *New York Times*, June 16, 2012. www.nytimes.com.

[61] Steve Kroft. “The Data Brokers: Selling Your Personal Information.” *60 Minutes*, March 9, 2014. 14:22. www.cbsnews.com.

[62] “How Deep Are Your Pockets?” *Economist*, June 30, 2012.

[63] Joseph Walker. “Data Mining to Recruit Sick People.” *Wall Street Journal*, December 17, 2013. www.wsj.com.

[64] Jeanne Cummings. “Rove’s Patented Strategies Will Endure.” *Politico*, August 13, 2007. www.politico.com.

[65] Christina Newberry. “Social Media Sentiment Analysis: Tools and Tips for 2023.” *Hootsuite*, September 29, 2022. https://blog.hootsuite.com/social-media-sentiment-analysis-tools/.

[66] “Number of Employers Passing on Applicants Due to Social Media Posts Continues to Rise, According to

New CareerBuilder Survey" (press release). CareerBuilder, June 26, 2014. www.careerbuilder.com.

[67] "Untangling the Social Web." *Economist Technology Quarterly*, 16–17, September 4, 2010.

[68] "Tools to Help You Control Your Privacy and Security on Facebook." Facebook (Web site). Accessed June 10, 2018. www.facebook.com/privacy/.

[69] Arvind Narayanan and Vitaly Shmatikov. "Robust De-anonymization of Large Sparse Datasets." *2008 IEEE Symposium on Security and Privacy*, May 18–21, 2008.

[70] Neil Hunt. "Netflix Prize Update." *The Official Netflix Blog*, March 12, 2010. blog.netflix.com.

[71] Tom Zeller Jr. "AOL Executive Quits After Posting of Search Data—Technology—International Herald Tribune." *New York Times*, August 22, 2006. www.nytimes.com.

[72] Michael Arrington. "AOL Proudly Releases Massive Amounts of Private Data." *TechCrunch*, August 6, 2006. techcrunch.com.

[73] Michael Barbaro and Tom Zeller Jr. "A Face Is Exposed for AOL Searcher No. 4417749." *New York*

Times, August 9, 2006.

[74] Dawn Kawamoto. "AOL Apologizes for Release of User Search Data." CNET (Web site), August 9, 2006. www.cnet.com.

[75] Nicholas Carlini, Florian Tramèr, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Úlfar Erlingsson, Alina Oprea, and Colin Raffel. "Extracting Training Data from Large Language Models." arXiv:2012.07805, June 15, 2021. https://arxiv.org/abs/2012.07805.

[76] Ann Cavoukian and Don Tapscott. *Who Knows: Safeguarding Your Privacy in a Networked World*. McGraw-Hill, New York, NY, 1996.

[77] Facebook. "Leading Websites Offer Facebook Beacon for Social Distribution" (press release). November 6, 2007. www.facebook.com.

[78] Ellen Nakashima. "Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy." *Washington Post*, November 30, 2007.

[79] Farhad Manjoo. "Facebook Finally Lets Users Turn Off Privacy-Invading Ads." *Salon* (Web site), December 6,

2007. www.salon.com.

[80] "Malls Stop Tracking Shoppers' Cell Phones." *CNNMoney*, November 28, 2011. money.cnn.com.

[81] Arun Thampi. "Path Uploads Your Entire iPhone Address Book to Its Servers." *mclov.in* (blog), February 8, 2012. mclov.in.

[82] Nick Bilton. "Disruptions: So Many Apologies, So Much Data Mining." *New York Times*, February 12, 2012.

[83] Nicole Perlroth and Nick Bilton. "Mobile Apps Take Data Without Permission." *New York Times*, February 15, 2012.

[84] Jenna Wortham and Nick Bilton. "What Instagram's New Terms of Service Mean for You." *New York Times*, December 17, 2012.

[85] Nicole Perlroth and Jenna Wortham. "Instagram's Loss Is a Gain for Its Rivals." *New York Times*, December 20, 2012.

[86] Kevin Systrom. "Updated Terms of Service Based on Your Feedback." Instagram, December 2012. blog.instagram.com.

[87] Ben Quinn and Jasper Jackson. “Daily Telegraph to Withdraw Devices Monitoring Time at Desk After Criticism.” *The Guardian*, January 11, 2016. https://www.theguardian.com/media/2016/jan/11/daily-telegraph-to- withdraw-devices-monitoring-time-at-desk-after-criticism.

[88] Nicholas Confessore and Danny Hakim. “Data Firm Says ‘Secret Sauce’ Aided Trump; Many Scoff.” *New York Times*, March 6, 2017. www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html.

[89] Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr. “How Trump Consultants Exploited the Facebook Data of Millions.” *New York Times*, March 27, 2018. www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[90] Paul Lewis and Julia Carrie Wong. “Facebook Employs Psychologist Whose Firm Sold Data to Cambridge Analytica.” *Guardian*, March 18, 2018. www.theguardian.com/news/2018/mar/18/facebook-cambridge-analytica-joseph-chancellor-gsr.

[91] Mattathias Schwartz. “Facebook Failed to Protect 30 Million Users from Having Their Data Harvested by Trump Campaign Affiliate.” *The Intercept* (Web site), March 30, 2018. theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users- from-having-their-data-harvested-by-trump-campaign-affiliate/.

[92] Issie Laposky. “Facebook Exposed 87 Million Users to Cambridge Analytica.” *Wired*, April 4, 2018. www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/.

[93] Paul Grewal. “Suspending Cambridge Analytica and SCL Group from Facebook.” Facebook (Web site), March 17, 2018. newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

[94] Josh Constine. “Facebook Is Shutting Down Its API for Giving Your Friends’ Data to Apps.” TechCrunch (Web site), April 28, 2015. techcrunch.com/2015/04/28/facebook-api-shut-down/.

[95] “Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users.” *Guardian*, December 11, 2015. www.theguardian.com/us-

news/2015/dec/11/senatorted-cruz-president-campaign-facebook-user-data.

[96] Michael Kranish. “Trump’s Plan for a Comeback Includes Building a ‘Psychographic’ Profile of Every Voter.” *Washington Post*, October 27, 2016. www.washingtonpost.com.

[97] Tony Romm. “Mark Zuckerberg Just Survived 10 Hours of Questioning by Congress.” *Washington Post*, April 11, 2018. www.washingtonpost.com.

[98] Nicholas Confessore and Matthew Rosenberg. “Cambridge Analytica to File for Bankruptcy After Misuse of Facebook Data.” *New York Times*, May 2, 2018. www.nytimes.com/2018/05/02/us/politics/cambridge-analytica-shut-down.html.

[99] Steve Lohr. “How Privacy Vanishes Online.” *New York Times*, March 16, 2010.

[100] Stewart Deck. “Legal Thumbs-Up for Raytheon Employee Suit; Privacy Groups Chilled by ISP Subpoenas.” *Computerworld*, April 12, 1999.

[101] Jessica Guynn. “Google Glass Sees All – and That Raises Privacy Concerns.” *Los Angeles Times*, August

9, 2013.

[102] Laura Clark Brown. “Third-Party-Privacy-Case-Studies.” *Southern Historical Collection 2009 Symposia Wiki*, Chapel Hill, North Carolina, February, 2009. shc2009\protect\discretionary\char\hyphenchar\fontsymposia.p

Chapter 6

Privacy and the Government

6.1 Introduction

POLICE IN NEW YORK CITY ARRESTED JALANI HENRY, A BLACK PERSON, on two counts of attempted murder in 2012. Henry did not have a criminal record, but he was denied bail because the likes and group photos he had posted on social media enabled the Manhattan District Attorney to portray him as a member of a violent gang. Henry spent 19 months in the violent Rikers Island jail before his case was finally dismissed for lack of evidence [**1**].

In 2017 the US government began purchasing cellphone location data from private company Venntel. The Department of Homeland Security said its Immigration and Customs Enforcement division was using some of the data to identify immigrants entering the United States illegally. Cellphone location data also helped ICE discover a drug-smuggling tunnel under the US–Mexico border ending in a closed Kentucky Fried Chicken restaurant near San Luis, Arizona. The American Civil Liberties Union argued the data purchase was a circumvention of US residents' Fourth Amendment rights against unreasonable searches and seizures [**2**]. Alan Butler, general counsel of the Electronic Privacy Information Center, said, "This is a classic situation where

creeping commercial surveillance in the private sector is now bleeding directly over into government" [3].

Amazon offers video doorbells and other home security products under its Ring subsidiary. If a police department in the United States seeks video footage from a homeowner's camera, it is supposed to obtain a court warrant or the permission of the homeowner. A 2019 investigation by journalists revealed that Ring was coaching police departments on how to overcome homeowner reluctance and gain their permission to see their video footage without a warrant. Police departments requested Ring videos over 20,000 times in 2020. In a 2022 response to US senator Ed Markey, Ring admitted that it sometimes provided videos to police departments without a warrant or the owner's consent, in "cases involving imminent danger of death or serious injury to any person" [4].

In this chapter we consider the impact that federal, state, and local governments in the United States have had on the information privacy of US residents. The word "privacy" does not even appear in the Constitution of the United States, and it has been difficult for the legislative, executive, and judicial branches of government to find the right compromise between demands for privacy and competing concerns. We

survey legislation designed to protect the information privacy of individuals as well as legislation allowing law-enforcement agencies to collect information about individuals in an effort to prevent criminal or terrorist activities. We look at famous examples from US history in which governmental agencies engaged in illegal activities under the banner of protecting public safety and/or national security, and we see how the US Supreme Court gradually shifted its view of information privacy rights over time.

)

To organize our presentation, we will use the taxonomy of privacy proposed by Daniel Solove [5].[1] Solove groups privacy-related activities into four categories:

1. *Information collection* refers to activities that gather personal information. We discuss issues related to information collection by the government in Sections 6.2 through 6.6.

2. *Information processing* refers to activities that store, manipulate, and use personal information that has been collected. Sections 6.7 through 6.9 focus on the information-processing category.

3. *Information dissemination* refers to activities that spread personal information. Section 6.10 provides

examples of laws designed to restrict information dissemination by private organizations, as well as legal ways in which information held by the government can be disseminated.

4. *Invasion* refers to activities that intrude upon a person's daily life, interrupt a person's solitude, or interfere with someone's decision making. In Section 6.11 we survey government actions to limit intrusion by other organizations, as well as government programs that can be seen as intrusive.

We consider each of these categories in turn, examining how federal, state, and local governments in the United States have addressed the often competing interests of protecting personal privacy and promoting the common good.

eproduced by permission of the publisher from *Understanding Privacy* by aniel J. Solove, p. 103. Cambridge, MA: Harvard University Press. Copyrigh)08 by the President and Fellows of Harvard College.

6.2 US Legislation Restricting Information Collection

This section gives three examples of federal legislation that limits the amount of information private entities can collect from individuals.

6.2.1 Employee Polygraph Protection Act

The Employee Polygraph Protection Act of 1988 (EPPA) prohibits most private employers from using lie-detector tests under most situations. An employer may not require or even request a job applicant or employee to take a lie-detector test, and an employee who refuses to take a lie-detector test cannot suffer any retaliation.

The law has several important exceptions. Pharmaceutical companies and security firms may administer polygraph tests to job applicants in certain job categories. Employers who have suffered an economic loss, such as theft, may administer polygraph tests to employees whom they reasonably suspect were involved. Most significantly, EPPA does not apply to federal, state, and local governments.

6.2.2 Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA), which went into effect in 2000, is designed to reduce the amount of information gathered from children using the Internet. According to COPPA, online services must obtain parental consent before collecting any information from children 12 years old and younger.

In 2022 Epic Games paid a $275 million settlement to the US government. The Federal Trade Commission had flagged Epic Games for violating the Children's Online Privacy Protection Act by collecting information from children playing Fortnite without first obtaining their parent's consent [6].

6.2.3 Genetic Information Nondiscrimination Act

The Genetic Information Nondiscrimination Act of 2008 is designed to prevent discrimination in the areas of medical benefits and employment based on genetic information. It prohibits health insurance companies and health plan administrators from requesting genetic information from individuals or their family members, and it forbids them from using genetic information when making decisions about coverage, rates, or preexisting conditions. It also prohibits most employers from taking genetic information into account when making hiring, firing, promotion, or any other decisions related to the terms of employment. The law does not extend these nondiscrimination protections to life insurance, disability insurance, or long-term care insurance, and it does not apply to employers with fewer than 15 employees [7].

6.2 US Legislation Restricting Information Collection

This section gives three examples of federal legislation that limits the amount of information private entities can collect from individuals.

6.2.1 Employee Polygraph Protection Act

The Employee Polygraph Protection Act of 1988 (EPPA) prohibits most private employers from using lie-detector tests under most situations. An employer may not require or even request a job applicant or employee to take a lie-detector test, and an employee who refuses to take a lie-detector test cannot suffer any retaliation.

The law has several important exceptions. Pharmaceutical companies and security firms may administer polygraph tests to job applicants in certain job categories. Employers who have suffered an economic loss, such as theft, may administer polygraph tests to employees whom they reasonably suspect were involved. Most significantly, EPPA does not apply to federal, state, and local governments.

6.2.2 Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA), which went into effect in 2000, is designed to reduce the amount of information gathered from children using the Internet. According to COPPA, online services must obtain parental consent before collecting any information from children 12 years old and younger.

In 2022 Epic Games paid a $275 million settlement to the US government. The Federal Trade Commission had flagged Epic Games for violating the Children's Online Privacy Protection Act by collecting information from children playing Fortnite without first obtaining their parent's consent [6].

6.2.3 Genetic Information Nondiscrimination Act

The Genetic Information Nondiscrimination Act of 2008 is designed to prevent discrimination in the areas of medical benefits and employment based on genetic information. It prohibits health insurance companies and health plan administrators from requesting genetic information from individuals or their family members, and it forbids them from using genetic information when making decisions about coverage, rates, or preexisting conditions. It also prohibits most employers from taking genetic information into account when making hiring, firing, promotion, or any other decisions related to the terms of employment. The law does not extend these nondiscrimination protections to life insurance, disability insurance, or long-term care insurance, and it does not apply to employers with fewer than 15 employees [7].

6.3 Information Collection by the Government

In the previous section we considered ways in which the federal government has restricted the amount of information that private organizations can collect about individuals. In this section we look at ways in which the federal government itself has collected vast amounts of sensitive information about its citizens.

6.3.1 Census Records

In order to ensure each state has fair representation in the House of Representatives, the United States Constitution requires the government to perform a census every 10 years.

The first census of 1790 had six questions. It asked for the name of the head of the household and the number of persons in each of the following categories: free white males at least 16 years old; free white males under 16 years old; free

white females; all other free persons (by sex and color); and enslaved Black people.

As time passed, the number of questions asked during the census increased. The 1820 census determined the number of people engaged in agriculture, commerce, and manufacturing. The 1840 census had questions regarding school attendance, illiteracy, and occupations. In 1850 census takers began asking questions about taxes, schools, crime, wages, and property values.

The 1940 census is notable because for the first time statistical sampling was put to extensive use. A random sample of the population, about 5 percent of those surveyed, received a longer form with more questions. The use of sampling enabled the Census Bureau to produce detailed demographic profiles without substantially increasing the amount of data it needed to process.

Today the Census Bureau only uses a single short form when conducting the decennial census. It gathers more detailed information on a continuous basis through the American Community Survey. This program mails a questionnaire with more than 50 questions to 3 million addresses per year. Questions include the following:

- What is this person's ancestry or ethnic origin?
- Does this person speak a language other than English at home?
- How many times has this person been married?
- How did this person usually get to work last week?
- Which fuel is used most for heating this house, apartment, or mobile home?

According to federal law, the Census Bureau is supposed to keep confidential the information it collects. However, in times of national emergency, the Census Bureau has revealed its information to other agencies. During World War I, the Census Bureau provided the names and addresses of young men to the military, which was searching for draft resisters. After Japan's attack on Pearl Harbor, the Census Bureau provided the Justice Department with information from the 1940 census about the general location of Japanese Americans. The Army used this information to round up Japanese Americans and send them to internment camps (Figure 6.1).

Figure 6.1

After Japan's attack on Pearl Harbor, the Army used information illegally obtained from the Census Bureau to round up Japanese Americans and send them to internment camps.

6.3.2 Internal Revenue Service Records

The United States enacted a national income tax in 1862 to help pay for expenses related to the Civil War. In 1872 the income tax was repealed. Congress resurrected the national income tax in 1894, but a year later the US Supreme Court ruled it unconstitutional. The Sixteenth Amendment to the Constitution, ratified by the states in 1913, gives the United States government the power to collect an income tax. A national income tax has been in place ever since. The Internal Revenue Service (IRS) now collects about $2 trillion a year in taxes.

Your income tax form may reveal a tremendous amount of personal information about your income, your assets, the organizations to which you give charitable contributions, your medical expenses, and much more.

6.3.3 FBI National Crime Information Center 2000

The FBI National Crime Information Center 2000 (NCIC) is a collection of databases supporting the activities of federal, state, and local law enforcement agencies in the United States, the United States Virgin Islands, Puerto Rico, and Canada [8]. Its predecessor, the National Crime Information Center, was established by the FBI in January 1967 under the direction of J. Edgar Hoover.

When it was first activated, the NCIC consisted of 356,784 records in five databases: stolen automobiles, stolen license plates, stolen or missing guns, other stolen items, and missing persons. Today the National Crime Information Center consists of 21 databases, which include such categories as wanted persons, criminal histories, people incarcerated in federal prisons, convicted sex offenders, unidentified persons, people believed to be a threat to the president, foreign

fugitives, violent gang members, and suspected terrorists. More than 90,000 law enforcement agencies have access to these data files. The NCIC processes about 14 million requests for information each day. For example, a police officer can initiate an NCIC search during a traffic stop to find out if the vehicle is stolen or there is a warrant out for the driver, and the system "responds instantly" [9].

The FBI points to the following successes of the NCIC:

- Investigating the assassination of Dr. Martin Luther King Jr., the NCIC provided the FBI with the information it needed to link a fingerprint on the murder weapon to James Earl Ray.
- About an hour after the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma state trooper Charles Hanger pulled over a Mercury Marquis with no license plates. Seeing a gun in the back seat of the car, Hanger arrested the driver—Timothy McVeigh—on the charge of transporting a loaded firearm in a motor vehicle. He took McVeigh to the county jail, and the arrest was duly entered into the NCIC database. Two days later, when federal agents ran McVeigh's name through the NCIC, they saw Hanger's arrest record. FBI agents reached the jail just

before McVeigh was released (Figure 6.2). McVeigh was subsequently convicted of the bombing.

Figure 6.2

The National Crime Information Center facilitated the arrest of Timothy McVeigh for the 1995 bombing of the Federal Building in Oklahoma City. (Ralf-Finn Hestoft/Corbis Premium Historical/Getty Images)

Critics of the National Crime Information Center point out ways in which the existence of the NCIC has led to privacy violations of innocent people:

- Erroneous records can lead law enforcement agencies to arrest innocent persons.
- Innocent people have been arrested because their name is the same as that of someone listed in the arrest warrants database.
- The FBI has used the NCIC to keep records about people not suspected of any crime, such as opponents of

the Vietnam War.

- Corrupt employees of law enforcement organizations with access to the NCIC have sold information to private investigators and altered or deleted records.
- People with access to the NCIC have illegally used it to search for criminal records on acquaintances or to screen potential employees, such as babysitters.

6.3.4 National Data Exchange

The National Data Exchange (N-DEx) is a database allowing thousands of US law enforcement agencies at the federal, state, and local level to share information. The N-DEx system complements the National Crime Information Center by containing incident reports, arrest reports, reports from pre-trial investigations, and information from correctional institutions. Access to information from a variety of sources helps crime investigators "connect the dots" [**10**]. The database contains more than 600 million records [**11**].

6.3.5 Closed-Circuit Television Cameras

The use of closed-circuit television cameras for video surveillance in the United States began in western New York in 1968. The small town of Olean installed a surveillance camera along its main business street in an effort to reduce crime. Within a year, more than 160 police chiefs from around the country visited Olean to learn more about their system [**12**]. Atlanta, Georgia, now has more video surveillance cameras than any other US city, with 1 camera for every 20 residents [**13**].

The number of surveillance cameras keeps increasing (Figure 6.3). New York City spent $201 million to install 3,000 closed-circuit security cameras in lower Manhattan. These surveillance cameras are connected to computer systems with sophisticated image-scanning software that can sound alarms if someone leaves an unattended package. The cameras are part of a larger network of sensors that also includes license-plate readers and radiation detectors [**14**].

Figure 6.3

After the Boston Marathon bombing, images from surveillance cameras played an important role in the apprehension of the suspects

The New York Civil Liberties Union has expressed opposition to the large increase in security cameras, saying they represent a violation of privacy and will not prevent terrorist attacks. The associate legal director of the NYCLU, Christopher Dunn, said, “Our main concern is that it’s unlike most police activity, which is focused on people who are suspected of unlawful activity. In fact, 99.9 percent of people who are captured in the system are just going to be people walking around, going about their business” [**14**].

Some critics point to the United Kingdom as proof that surveillance cameras cannot guarantee public safety. There are between 4 and 6 million surveillance cameras in Britain, one for every 14 people. It has been estimated that the average Briton is caught on camera an average of 300 times per day [**15**]. Still, the presence of all these cameras did not

prevent the suicide bombings on the London public transport system in 2005 [16]. Some experts have reached the conclusion that closed-circuit television cameras are “largely ineffective” for crime prevention [17].

6.3.6 Police Misuse of Facial Recognition Systems

Facial recognition software is now commonly used by police in the United States. In a typical investigation, an officer will capture a still image from a security camera video or another source, select which database to run the image against, crop the still image to be more like the photos in the selected database, run the search, and review the list of possible matches. Companies creating the facial recognition software and the police departments using the software state that a facial recognition match should be treated only as a lead and does not provide probable cause to make an arrest. However, police officers have in fact relied solely upon positive matches from facial recognition software to make arrests. When they do so, they are exhibiting a bias against people of color because the false positive rate for face recognition systems is significantly higher for darker-skinned individuals than for lighter-skinned individuals [18]. In several cases, innocent

Black men have been jailed and have faced charges when the only piece of evidence against them was a match from a facial recognition system [19].

Between 2019 and 2021, about two dozen state or local governments in the United States passed laws banning the use of facial recognition technology by police departments and other government agencies. However, concerns about rapidly rising crime rates caused some of these governments to drop their bans only one or two years later [20].

6.3.7 License-Plate Scanners

More than 70 percent of police departments in the United States make use of scanners that read license-plate numbers of passing cars and record the time and location where each car was spotted. License-plate scanners, typically mounted on police cars, parking enforcement vehicles, road signs, toll gates, or bridges, track the movements of millions of automobiles every year. Police credit license-plate scanners with helping them find stolen vehicles and solve criminal cases [21].

The American Civil Liberties Union has protested the widespread collection of data about citizens who are not suspected of committing any crime. In one widely publicized incident, police in New York City drove unmarked cars equipped with license-plate scanners to record the license-plate numbers of cars parked near a mosque in Queens [22].

Several states have passed legislation restricting the use of license-plate scanners and/or putting limits on how long police can retain the scans. For example, New Hampshire prohibits the use of license-plate scanners, with several exceptions, including toll-booths, bridges, and police investigations approved on a case-by-case basis. A California statute requires the California Highway Patrol to purge scans after 60 days, except for scans being used as evidence in a criminal investigation, and it prohibits the sale or distribution of license-plate data to any non–law enforcement organizations [23].

6.3.8 Police Drones

Hundreds of police and sheriff's departments in the United States have begun operating unmanned drones (Figure 6.4). Police drones are nothing like the large Predator drones used by the US military; Federal Aviation Administration rules

require that drones used by the police weigh no more than 25 pounds, fly no higher than 400 feet, and be flown during daylight within view of the operator [24]. Possible uses of the small drones include searching for missing persons, surveying storm damage to isolated neighborhoods, controlling illegal immigration, pursuing people who are fugitives, and performing surveillance at large public gatherings [25].

Figure 6.4

Some police departments have acquired small unmanned drones to serve as surveillance platforms.

(Jarp5/123RF)

Some uses of police drones are supported by the public, but others are not. In a poll conducted by Monmouth University, 66 percent of Americans expressed privacy concerns related to the use of unmanned drones with high-tech cameras by US law enforcement agencies, and 67 percent opposed the use of

drones to issue speeding tickets, but 80 percent supported the use of drones in search-and-rescue missions [**26**].

Numerous cities and states are currently debating what controls, if any, should be placed on the use of drones by police. Should police be required to get a search warrant before deploying a drone, or should they be able to use a drone to collect the evidence they need to get a search warrant? Seattle police purchased two drones, but after a strong public protest, Mayor Mike McGinn ordered the drones to be sent back to the manufacturer [**25**]. Florida, Virginia, and Idaho have passed laws prohibiting the use of police drones for crowd surveillance at public events [**27**].

6.4 Covert Government Surveillance

We now turn to ways in which the US government has collected information in order to detect and apprehend suspected criminals or to improve national security. Because the individuals being observed are suspected of wrongdoing, they are not alerted or asked for permission before the surveillance begins.

Does covert surveillance violate any of the rights of a citizen? The most relevant statement in the US Constitution is the Fourth Amendment.

Fourth Amendment to the United States Constitution

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Before the American Revolution, English agents in pursuit of smugglers made use of *writs of assistance*, which gave them authority to enter any house or building and seize any prohibited goods they could find. This activity drew the ire of the colonists. It is not surprising, then, that a prohibition against unreasonable searches and seizures appears in the Bill of Rights.

The position of the US Supreme Court with respect to covert electronic surveillance has changed over time. Let's see how the Supreme Court's position evolved.

6.4.1 Wiretaps and Bugs

Wiretapping refers to the interception of a telephone conversation. (The term is somewhat anachronistic, because many telephone conversations are no longer transmitted over wires.) Wiretapping has been taking place ever since the 1890s, when telephones became commonly used. The state of New York made wiretapping a felony in 1892, but the police in New York City ignored the law and continued the practice of wiretapping. Until 1920, the New York City police listened to conversations between lawyers and clients, doctors and patients, and priests and penitents. On several occasions the police even tapped the trunk lines into hotels and listened to the telephone conversations of all the hotel guests [28].

Olmstead v. United States

Wiretapping was a popular tool for catching bootleggers during Prohibition (1919–1933). The most famous case involved Roy Olmstead, who ran a $2-million-a-year bootlegging business in Seattle, Washington. Without a warrant, federal agents tapped Olmstead's phone and collected enough evidence to convict him. Although wiretapping was illegal under Washington law, the state court allowed evidence obtained through the wiretapping to be admitted. Olmstead appealed all the way to the US Supreme Court. His lawyer argued that the police had

violated Olmstead's right to privacy by listening in on his telephone conversations. He also argued that the evidence should be thrown out because it was obtained without a search warrant [**28, 29**].

In a 5–4 decision, the Supreme Court ruled in *Olmstead v. United States* that the Fourth Amendment protected tangible assets alone. The federal agents did not "search" a physical place; they did not "seize" a physical item. Hence the Fourth Amendment's provision against warrantless search and seizure did not apply. Justice Louis Brandeis (mentioned in Section 5.2.3) was one of the four judges siding with Olmstead. In his dissenting opinion, Brandeis argued that the protections afforded by the Bill of Rights ought to extend to electronic communications as well. He wrote:

> **Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny**

> **instruments of tyranny and oppression when compared with wiretapping.** [30]

Congress Makes Wiretapping Illegal

The public and the press were critical of the Supreme Court decision. Since the Court had ruled that wiretapping was constitutional, those interested in prohibiting wiretapping focused their efforts on the legislative branch. In 1934 the US Congress passed the Federal Communications Act, which (among other things) made it illegal to intercept and reveal wire communications. Three years later the Supreme Court used the Federal Communications Act to reverse its position on warrantless wiretaps. In *Nardone v. United States*, the Court ruled that evidence obtained by federal agents from warrantless wiretaps was inadmissible in court. In another decision, *Weiss v. United States*, it ruled that the prohibition on wiretapping applied to intrastate as well as interstate telephone calls. Subsequently, the attorney general announced that the FBI would cease wiretapping [28, 29].

FBI Continues Secret Wiretapping

After World War II broke out in Europe, FBI director J. Edgar Hoover pressed to have the ban on wiretapping

withdrawn. The position of the Department of Justice was that the Federal Communications Act simply prohibited intercepting *and* revealing telephone conversations. In the Justice Department's view, it was permissible to intercept conversations as long as they were not revealed to an agency outside the federal government. President Roosevelt agreed to let the FBI resume wiretapping in cases involving national security, though he asked that the wiretaps be kept to a minimum and limited as much as possible to aliens [28].

Because it knew evidence obtained through wiretapping was inadmissible in court, the FBI began maintaining two sets of files: the official files that contained legally obtained evidence, and confidential files containing evidence obtained from wiretaps and other confidential sources. In case of a trial, only the official file would be released to the court [28].

The FBI was supposed to get permission from the Department of Justice before installing a wiretap, but in practice it did not always work that way. During his 48-year reign as director of the FBI, J. Edgar Hoover routinely engaged in political surveillance, tapping the telephones of senators, congressional representatives, and Supreme Court justices. The information the FBI collected on these figures had great political value, even if the recordings revealed no

criminal activity. There is evidence Hoover used information gathered during this surveillance to discredit members of Congress who were trying to limit the power of the FBI [28].

Charles Katz v. United States

A **bug** is a hidden microphone used for surveillance. In a series of decisions, the US Supreme Court gradually came to an understanding that citizens should also be protected from all electronic surveillance conducted without warrants, including bugs. The key decision was rendered in 1967. Charles Katz used a public telephone to place bets. The FBI placed a bug on the outside of the telephone booth to record Katz's telephone conversations. With this evidence, Katz was convicted of illegal gambling. The Justice Department argued that since it placed the microphone on the outside of the telephone booth, it did not intrude into the space occupied by Katz [28]. In *Charles Katz v. United States*, the Supreme Court ruled in favor of Katz. Justice Potter Stewart wrote that "the Fourth Amendment protects people, not places" [31]. Katz entered the phone booth with the reasonable expectation that his conversation would not be heard, and what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" [31].

6.4.2 Operation Shamrock

During World War II, the US government censored all messages entering and leaving the country, meaning US intelligence agencies had access to all telegram traffic. At the end of the war, the censorship bureaucracy was shut down, and the Signal Security Agency (predecessor to the National Security Agency) wanted to find a new way to get access to telegram traffic. It contacted Western Union Telegraph Company, ITT Communications, and RCA Communications, and asked them to allow it to make photographic copies of all foreign government telegram traffic that entered, left, or transited the United States. In other words, the Signal Security Agency asked these companies to break federal law in the interests of national security. All three companies agreed to the request. The Signal Security Agency gave this intelligence-gathering operation the name "Shamrock."

When the National Security Agency (NSA) was formed in 1952, it inherited Operation Shamrock. The sophistication of the surveillance operation took a giant leap forward in the 1960s, when the telegram companies converted to computers. Now the contents of telegrams could be transmitted

electronically to the NSA, and the NSA could use computers to search for key words and phrases.

In 1961 Robert Kennedy became the new attorney general of the United States, and he immediately focused his attention on organized crime. Discovering that information about mobsters was scattered piecemeal among the FBI, IRS, Securities and Exchange Commission (SEC), and other agencies, he convened a meeting in which investigators from all of these agencies could exchange information. The Justice Department gave the names of hundreds of alleged crime figures to the NSA, asking that these figures be put on its "watch list." Intelligence gathered by the NSA contributed to several prosecutions.

Also during the Kennedy administration, the FBI asked the NSA to put on its watch list the names of US citizens and companies doing business with Cuba. The NSA sent information gathered from intercepted telegrams and international telephone calls back to the FBI.

During the Vietnam War, the Johnson and Nixon administrations hypothesized that foreign governments were controlling or influencing the activities of American groups opposed to the war. They asked the NSA to put the names of war protesters on its watch list. Some of the people placed on

the watch list included the Reverend Dr. Martin Luther King Jr., the Reverend Ralph Abernathy, Black Panther leader Eldridge Cleaver, pediatrician Dr. Benjamin Spock, folksinger Joan Baez, and actress Jane Fonda.

In 1969 President Nixon established the White House Task Force on Heroin Suppression. The NSA soon became an active participant in the war on drugs, monitoring the phone calls of people put on its drug watch list. Intelligence gathered by the NSA led to convictions for drug-related crimes.

Facing hostile congressional and press scrutiny, the NSA called an end to Operation Shamrock in May 1975 [**32**].

6.4.3 Carnivore Surveillance System

The FBI developed the Carnivore system in the late 1990s to monitor Internet traffic, including email messages. The system itself consisted of a Windows PC and packet-sniffing software capable of identifying and recording packets originating from or directed to a particular IP address. Armed with a search warrant, the FBI would set up its Carnivore system at the suspect's Internet service provider [**33**].

In 2000 the Justice Department demanded that Earthlink, an Internet service provider, allows the FBI to use Carnivore without a warrant. Earthlink filed a legal challenge questioning the FBI's authority to do this under the Electronic Communications Privacy Act, but a US District Court ruled against Earthlink [**34, 35**].

Between 1998 and 2000 the FBI used the Carnivore system about 25 times. In late 2001 the FBI stopped using Carnivore, replacing it with commercial software capable of performing the same function [**36**].

6.4.4 Covert Activities After 9/11

The September 11, 2001, attacks on the World Trade Center and the Pentagon spawned new, secret intelligence-gathering operations within the United States. The same question emerged after each activity became public knowledge: Is it constitutional?

NSA Wiretapping

Early in 2002 the Central Intelligence Agency captured several top al-Qaeda members, along with their personal

computers and cell phones. The CIA recovered telephone numbers from these devices and provided them to the NSA. The NSA was eager to eavesdrop on these telephone numbers, hoping to gather information that could be used to disrupt future terrorist attacks. President Bush signed a presidential order allowing the NSA to eavesdrop on international telephone calls and international emails initiated by people living inside the United States, without first obtaining a search warrant [37].

The list of persons being monitored gradually expanded, as the NSA followed connections from the original list of telephone numbers. At any one time, the NSA eavesdropped on up to 500 people inside the United States, including US citizens, permanent residents of the United States, and visitors from other countries. The NSA also monitored another 5,000 to 7,000 people living outside the United States at any one time [37].

Sources told the *New York Times* that the surveillance program had foiled at least two al-Qaeda plots: Ohio truck driver Iyman Faris's plan to "bring down the Brooklyn Bridge with blowtorches" and another scheme to bomb British pubs and train stations. Civil libertarians and some members of Congress objected to the program, arguing that

warrantless wiretapping of American citizens violated the Fourth Amendment to the US Constitution [37].

Talon Database

The US Department of Defense created the Threat and Local Observation Notices (TALON) database in 2003. The purpose of the database was to collect reports of suspicious activities or terrorist threats near military bases. These reports were submitted by military personnel or civilians and then assessed by Department of Defense experts as either "credible" or "not credible."

In December 2005, *NBC News* reported that the database contained reports on antiwar protests occurring far from military bases [38]. In July 2006, the Servicemembers Legal Defense Network reported that the TALON database contained emails from students at Southern Connecticut State University, the State University of New York at Albany, the University of California, Berkeley, and William Paterson University of New Jersey, who were planning protests against on-campus military recruiting [39].

The Department of Defense removed many of these reports from TALON after conducting an in-house review that concluded the database should only contain information

related to terrorist activity. The American Civil Liberties Union asked Congress to take steps "to ensure that Americans may once again exercise their First Amendment rights without fear that they will be tracked in a government database of suspicious activities" [**40**]. In April 2007, the new Undersecretary of Defense for Intelligence recommended that the TALON program be terminated [**41**]. The TALON database was shut down on September 17, 2007 [**42**].

6.5 US Legislation Authorizing Wiretapping

As we have seen, the Federal Communications Act of 1934 made wiretapping illegal, and by 1967 the US Supreme Court had closed the door to wiretapping and bugging performed without a warrant (court order). After the Katz decision, police were left without any electronic surveillance tools in their fight against crime.

Meanwhile, the United States was in the middle of the Vietnam War. In 1968 the country was rocked by violent antiwar demonstrations and the assassinations of Martin Luther King Jr. and Robert F. Kennedy. Law enforcement agencies pressured Congress to allow wiretapping under some circumstances.

6.5.1 Title III

Congress responded by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III allows a

police agency that has obtained a court order to tap a phone for up to 30 days [28].

The government continued to argue that in cases of national security, agencies should be able to tap phones without a warrant. In 1972 the Supreme Court rejected this argument when it ruled that the Fourth Amendment forbids warrantless wiretapping, even in cases of national security [28].

6.5.2 Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978 (FISA) provides for judicial and congressional oversight of the government's covert surveillance of foreign governments and their agents. The law allows the president to authorize electronic surveillance of foreign nationals for up to one year without a court order, as long as there is little chance that the surveillance will reveal the contents of communications with any US citizens. If communications with US citizens are to be monitored, the government must get a court order from the FISA Court.

FISA was amended by the Protect America Act of 2007. This act allows the US government to wiretap communications

beginning or ending in a foreign country without oversight by the FISA Court.

In June 2013, the British newspaper the *Guardian* disclosed it had received a top-secret document outlining how the National Security Agency had obtained direct access to the servers at Google, Facebook, Yahoo, and other Internet giants [**43**]. (The document was provided by Edward Snowden, a former employee of NSA contractor Booz Allen Hamilton.) The secret program, called PRISM, enables the NSA to access stored information such as email messages and monitor live communications such as Skype and PalTalk conversations without first obtaining search warrants, when the NSA has a reasonable suspicion that the person being investigated is neither a US citizen nor a US resident. According to the secret document, the NSA gained access to the servers of Microsoft in 2007; Yahoo in 2008; Google and Facebook in 2009; YouTube in 2010; Skype and AOL in 2011; and Apple in 2012.

All the companies that responded to a request for information by the *Guardian* denied any knowledge of the PRISM program. The Obama administration provided the following statement: "The *Guardian* and *Washington Post* articles refer to collection of communications pursuant to

Section 702 of the Foreign Intelligence Surveillance Act. This law does not allow the targeting of any US citizen or of any person located within the United States" [43].

6.5.3 Electronic Communications Privacy Act

Congress updated the wiretapping law in 1986 with the passage of the Electronic Communications Privacy Act (ECPA). The ECPA allows police to attach two kinds of surveillance devices to a suspect's phone line. If the suspect makes a phone call, a **pen register** displays the number being dialed. If the suspect gets a phone call, a **trap-and-trace device** displays the caller's phone number. While a court order is needed to approve the installation of pen registers and trap-and-trace devices, prosecutors do not need to demonstrate probable cause, and the approval is virtually automatic.

The ECPA also allows police to conduct **roving wiretaps**—wiretaps that move from phone to phone—if they can demonstrate the suspect is attempting to avoid surveillance by using many different phones [28].

6.5.4 Stored Communications Act

The Stored Communications Act, part of the Electronic Communications Privacy Act, has significant privacy implications related to the collection of email messages. Under this law, the government does not need a search warrant to obtain from an Internet service provider email messages more than 180 days old. In other words, when a computer user allows an Internet service provider to store their email messages, the user is giving up the expectation of privacy of that information [**44**].

In the past it had been understood that the government needed a court order to gain access to emails under 180 days old, but in 2010 the government asked Yahoo to turn over emails under 180 days old that had already been read by the recipient [**45**]. Yahoo challenged this request in federal court, supported by Google, the Electronic Frontier Foundation, and the Center for Democracy & Technology, and the government withdrew its demand for the emails.

Nearly 50 companies and privacy rights organizations, including AOL, the American Civil Liberties Union, the

American Library Association, AT&T, Consumer Action, the Electronic Frontier Foundation, Facebook, Google, IBM, Intel, and Microsoft, have joined forces to form an organization called Digital Due Process, which is lobbying Congress to update the Electronic Communications Privacy Act. In the past Internet service providers simply transmitted email messages from senders to recipients. Today most Internet service providers supply convenient long-term storage of their customers' emails, and millions of customers take advantage of this service to hold their messages indefinitely. With the advent of cloud computing, companies such as Amazon, Google, and Microsoft are storing sensitive documents and other materials that in the past would have been held on personal computers. The view of the Digital Due Process coalition is that the government should not be able to obtain an email message, document, or photo from an Internet or cloud service provider without a proper search warrant [**46**].

6.5.5 Communications Assistance for Law Enforcement Act

The implementation of digital phone networks interfered with the wiretapping ability of the FBI and other organizations. In response to these technological changes, Congress passed the Communications Assistance for Law Enforcement Act of 1994 (CALEA), also known as the Digital Telephony Act. This law required that networking equipment used by phone companies be designed or modified so that law enforcement agencies can trace calls, listen in on telephone calls, and intercept email messages. CALEA thereby ensured that court-ordered wiretapping would still be possible even as new digital technologies were introduced.

CALEA left unanswered many important details about the kind of information the FBI would be able to extract from digital phone calls. The precise requirements were to be worked out between the FBI and industry representatives. The FBI asked for many capabilities, including the ability to intercept digits typed by the caller after the phone call was placed. This feature would let it catch credit card numbers and bank account numbers, for example. In 1999 the FCC finally issued the guidelines, which included this capability and five more requested by the FBI [47]. Privacy rights organizations argued these capabilities went beyond the authorization of CALEA [48]. Telecommunications companies claimed that implementing these capabilities

would cost them billions of dollars [**49**]. Nevertheless, in August 2005, the FCC determined that Voice over Internet Protocol (VoIP) and certain other broadband providers would need to modify their systems as necessary so that law enforcement agencies could wiretap calls made using their services [**50**].

6.6 USA PATRIOT Act

On the morning of September 11, 2001, terrorists hijacked four passenger airliners in the United States and turned them into flying bombs. Two of the planes flew into New York's World Trade Center, a third hit the Pentagon, and the fourth crashed in a field in Pennsylvania. Soon after these attacks, which resulted in about 3,000 deaths and the destruction of the twin towers of the World Trade Center, the US Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, henceforth referred to as the Patriot Act [**51**]. The Patriot Act has raised many questions about the extent to which government agencies should be able to collect information about individuals in the United States without first obtaining a search warrant.

6.6.1 Provisions of the Patriot Act

The Patriot Act amended many existing laws. Its provisions fall into four principal categories:

1. Providing federal law enforcement and intelligence officials with greater authority to monitor communications
2. Giving the Secretary of the Treasury greater powers to regulate banks, preventing them from being used to launder foreign money
3. Making it more difficult for terrorists to enter the United States
4. Defining new crimes and penalties for terrorist activity

We focus on those provisions of the Patriot Act that most directly affect the privacy of persons living inside the United States.

The Patriot Act expands the kinds of information that law enforcement officials can gather with pen registers and trap-and-trace devices. It allows police to use pen registers on the Internet to track email addresses and URLs. The law does not require they demonstrate probable cause. To obtain a warrant, police simply certify that the information to be gained is relevant to an ongoing criminal investigation.

Law enforcement agencies seeking to install a wiretap or a pen register/trap-and-trace device have always been required to get a court order from a judge with jurisdiction over the location where the device was to be installed. The Patriot Act extends the jurisdiction of court-ordered wiretaps to the entire country. A judge in New York can authorize the installation of a device in California, for example. The act also allows the nationwide application of court-ordered search warrants for terrorist-related investigations.

The Patriot Act broadened the number of circumstances under which roving surveillance can take place. Previously, roving surveillance could only be done for the purpose of law enforcement, and the agency had to demonstrate to the court that the person under investigation actually used the device to be monitored. The Patriot Act allows roving surveillance to be performed for the purpose of intelligence, and the government does not have to prove that the person under investigation actually uses the device to be tapped. Additionally, it does not require that the law enforcement agency report back to the authorizing judge regarding the number of devices monitored and the results of the monitoring.

Under the Patriot Act, law enforcement officials wishing to intercept communications to and from a person who has illegally gained access to a computer system do not need a court order if they have the permission of the owner of the computer system.

The Patriot Act allows courts to authorize law enforcement officers to search a person's premises without first serving a search warrant when there is "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse effect." Officers may seize property that "constitutes evidence of a criminal offense in violation of the laws of the United States," even if that offense is unrelated to terrorism.

6.6.2 National Security Letters

The Patriot Act expanded the use of National Security Letters, making it easier for the FBI to collect Internet, business, medical, educational, library, and church/mosque/synagogue records. To obtain a search warrant authorizing the collection of records about an individual, the FBI merely needs to issue a National Security

Letter stating that the records are related to an ongoing investigation. (The Patriot Act does specifically prohibit the FBI from investigating citizens solely on the basis of activities protected by the First Amendment.) A typical National Security Letter contains a gag order that forbids the letter's recipient from disclosing receipt of the letter. National Security Letters are controversial because, unlike warrants, they do not require the approval of a judge. That means there is no need for the FBI to show probable cause. Between 2003 and 2006, the FBI issued 192,499 National Security Letters [**52**]. The rate at which National Security Letters are issued has decreased markedly since then. In calendar year 2021 the FBI issued 12,362 National Security Letters [**53**].

National Security Letters have prompted several legal challenges by the American Civil Liberties Union (ACLU). One of these cases involved the Library Connection, a consortium of 26 libraries in Connecticut. In July 2005, the FBI sent a National Security Letter to the Library Connection, demanding records of a patron who had used a particular computer. This happened while Congress was debating reauthorization of the Patriot Act, and an important point in the debate was whether the FBI had actually attempted to use the Patriot Act to get information from libraries. The ACLU sought an emergency court order that

would have allowed representatives of the Library Connection to tell Congress that they had received a National Security Letter. In September 2005, a district court judge in Connecticut ruled that the National Security Letter's gag order violated the First Amendment to the US Constitution, but the executive branch continued to enforce it. In April 2006, six weeks after Congress had reauthorized the Patriot Act, the FBI dropped the gag order and its demand for the information. The ACLU hailed the government's decision as a victory "not just for librarians but for all Americans who value their privacy" [54].

6.6.3 Responses to the Patriot Act

Critics of the Patriot Act warn that its provisions give too many powers to the federal government. Despite language in the Patriot Act to the contrary, civil libertarians are concerned that law enforcement agencies may use their powers to reduce the rights of law-abiding Americans, particularly those rights expressed in the First and Fourth Amendments to the US Constitution.

First Amendment rights center around the freedom of speech and the free exercise of religion. We have seen that, in the

past, the FBI and the NSA used illegal wiretaps to investigate people who had expressed unpopular political views. In November 2003, the ACLU reported that public apprehension about the Patriot Act had led to a significant drop in attendance and donations at mosques [55].

Critics maintain that other provisions of the Patriot Act undermine the right against unreasonable searches and seizures guaranteed by the Fourth Amendment:

- The Patriot Act allows police to install Internet pen registers without demonstrating probable cause that the suspect is engaged in a criminal activity. By revealing the URLs of Web sites visited by a suspect, a pen register is a much more powerful surveillance tool on the Internet than it is on a telephone network.
- The Patriot Act allows for court orders authorizing roving surveillance that do not "particularly describe the place to be searched."
- It allows law enforcement agencies, under certain circumstances, to search homes and seize evidence without first serving a search warrant.
- It allows the FBI to obtain—without showing probable cause—a warrant authorizing the seizure of business,

medical, educational, and library records of suspects.

(Dana Summers/The Orlando Sentinel/TCA)

The Council of the American Library Association passed a resolution on the Patriot Act in January 2003. The resolution affirms every person's rights to inquiry and free expression. It "urges librarians everywhere to defend and support user privacy and free and open access to knowledge and information," and it "urges libraries to adopt and implement patron privacy and record retention policies" that minimize the collection of records about the activities of individual patrons [56]. More than four hundred cities and several states also passed anti–Patriot Act resolutions [57].

As alluded to earlier, the federal government issues about 12,000 National Security Letters every year [53]. Google is an obvious organization for law enforcement agencies to contact, given the significant amount of information it collects from individuals who use its search engine. In

December 2009, Google's CEO, Eric Schmidt, admitted Google is obliged to release personal data to law enforcement agencies. He said, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" [58].

6.6.4 Successes and Failures

According to Tom Ridge, former secretary of the Department of Homeland Security, the Patriot Act has helped the government in its fight against terrorism by allowing greater information sharing among law enforcement and intelligence agencies and by giving law enforcement agencies new investigative tools—"many of which have been used for years to catch mafia dons and drug kingpins" [59]. Terrorism investigations have led to charges being brought against 361 individuals in the United States. Of these, 191 have been convicted or pled guilty, including shoe-bomber Richard Reid and John Walker Lindh, who fought with the Taliban in Afghanistan. More than 500 individuals linked to the September 11th attacks have been removed from the United States. Terrorist cells in Buffalo, Seattle, Tampa, and Portland (the "Portland Seven")[2] have been broken up [59].

Unfortunately, a few innocent bystanders have been affected by the war against terrorism. A notable example is Brandon Mayfield.

During the morning rush hour on March 11, 2004, 10 bombs exploded on four commuter trains in Madrid, Spain, killing 191 people and wounding more than 2,000 others. The Spanish government retrieved a partial fingerprint from a bag of detonators, and the FBI linked the fingerprint to Brandon Mayfield, an attorney in Portland, Oregon [**60**].

Without revealing their search warrant, FBI agents secretly entered Mayfield's home multiple times, making copies of documents and computer hard drives, collecting 10 DNA samples, removing six cigarette butts for DNA analysis, and taking 355 digital photographs. The FBI also put Mayfield under electronic surveillance [**61**]. On May 6, 2004, the FBI arrested Mayfield as a material witness and detained him for two weeks. After the Spanish government announced that it had matched the fingerprints to Ouhnane Daoud, an Algerian national living in Spain, a judge ordered that Mayfield be released. The FBI publicly apologized for the fingerprint misidentification [**60**].

Mayfield said his detention was “an abuse of the judicial process” that “shouldn’t happen to anybody” [60]. He said, “I personally was subject to lockdown, strip searches, sleep deprivation, unsanitary living conditions, shackles and chains, threats, physical pain, and humiliation” [62]. The only evidence against Mayfield was a partial fingerprint match that even the Spanish police found dubious. Mayfield had not left the United States in more than a decade, and he had no connections with any terrorist organizations. Some civil rights groups suggest Mayfield was targeted by the FBI because of his religious beliefs. The affidavit that the FBI used to get an arrest warrant pointed out that Mayfield “had converted to Islam, is married to an Egyptian-born woman, and had once briefly represented a member of the Portland Seven in a child-custody case” [63]. Mayfield sued the US government for continuing to investigate him after the Spanish police had eliminated him as a suspect, and in November 2006, the government issued a formal apology and agreed to pay him $2 million [62].

6.6.5 Long-Standing NSA Access to Telephone Records

Beginning in 2011, two members of the Intelligence Committee of the US Senate, Ron Wyden of Oregon and Mark Udall of Arizona, repeatedly spoke out against domestic spying. In May 2011, Senator Wyden said, "I want to deliver a warning this afternoon: when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry" [**64**].

Two years later Americans began to learn what Senator Wyden was talking about. On June 5, 2013, the British newspaper the *Guardian* revealed that, based on a request from the FBI, the Foreign Intelligence Surveillance Court (FISC) had ordered Verizon to provide to the National Security Agency on a daily basis records of all of its customers' calls from April 25, 2013, to July 19, 2013 [**65**]. (Edward Snowden, mentioned in Section 6.5.2, was responsible for leaking the information to the *Guardian*.) These call records, also called **telephony metadata**, included the date and time of each telephone call, the location of the phone making the call, the duration of the conversation, and "other identifying information." Verizon was not asked to provide the contents of the conversations. The order from the FISC expressly prohibited Verizon from revealing to the public the FBI's request for this information. Opined the

Guardian, "These recent events reflect how profoundly the NSA's mission has transformed from an agency exclusively devoted to foreign intelligence gathering, into one that focuses increasingly on domestic communications" [**65**].

The Obama administration downplayed the revelation and held that the data collection was authorized under Section 215 of the Patriot Act. Deputy Press Secretary Josh Earnest said that the court orders for telephone records "are something that have been in place a number of years now" [**66**]. Dianne Feinstein, chair of the Senate Intelligence Committee, confirmed that position: "As far as I know, this is an exact three-month renewal of what has been the case for the past seven years" [**67**].

Senator Udall said, "This sort of wide-scale surveillance should concern all of us and is the kind of government overreach I've said Americans would find shocking" [**68**]. Former vice president Al Gore called the blanket order "obscenely outrageous" [**68**]. Republican congressman Jim Sensenbrenner, one of the authors of the Patriot Act, added, "I do not believe the broadly drafted FISA order is consistent with the requirements of the Patriot Act. Seizing phone records of millions of innocent people is excessive and un-American" [**68**].

In May 2015, a federal court in New York ruled that the NSA's program to collect customer telephone call records in bulk was illegal. According to the US Court of Appeals for the Second Circuit, it is unreasonable to interpret Section 215 of the Patriot Act as authorizing the bulk collection of telephone calling records [**69**].

Section 215 of the Patriot Act expired on June 1, 2015. Instead of renewing Section 215, Congress passed a reform of Section 215, called the USA Freedom Act. The USA Freedom Act put new restrictions on the government's surveillance activities. In particular, it shifted the bulk collection of telephone records to the phone companies and required government agencies to obtain a court order before accessing them [**70**].

ıe "Portland Seven" included six American Muslim men accused of attempti travel to Afghanistan to fight with the Taliban.

6.7 Regulation of Public and Private Databases

In this section we switch our focus to the information processing category of Solove's taxonomy of privacy. (Our coverage of issues related to information processing and the government continues through Section 6.9.)

Once organizations have collected information, they can manipulate and use it in a variety of ways, and some of these uses have privacy implications. We begin by describing the social conditions that led to the creation of the Code of Fair Information Practices and the passage of the Privacy Act of 1974. We then move on to legislation that regulates databases managed by private organizations.

6.7.1 Code of Fair Information Practices

In 1965 the director of the Bureau of the Budget commissioned a consulting committee, composed largely of economists, to look at problems caused by the decentralization of statistical data across many federal agencies. The Census Bureau, the Bureau of Labor Statistics, the Statistical Reporting Service, and the Economic Research Service of the Department of Agriculture maintained independent computer databases, making it impossible for economists and other social scientists to combine information about individuals. Carl Kaysen, the chair of the committee, described it this way:

> **It is becoming increasingly difficult to make informed and intelligent policy decisions on such questions in the area of poverty as welfare payments, family allowances, and the like, simply because we lack sufficient "dis-aggregated" information—breakdowns by the many relevant social and economic variables—that is both wide in coverage and readily usable. The information the Government does have is scattered among a dozen agencies, collected on a variety of not necessarily consistent bases, and not really accessible to any single group of policy-makers or research analysts. A test of the proposition, for example, that poor performance in school and poor prospects of social mobility are directly related to family size would require data combining information on at least family size and composition, family income, regional location, city size, school performance, and post-**

> **school occupational history over a period of years in a way that is simply not now possible, even though the separate items of information were all fed into some part of the Federal statistical system at some time. [71]**

After Kaysen's committee recommended the creation of a National Data Center, there was an immediate outcry from citizens and legislators expressing concerns about possible abuses of a massive, centralized government database containing detailed information about millions of Americans. The US House of Representatives created the Special Subcommittee on Invasion of Privacy, which held hearings about these issues [72].

In the early 1970s, Elliot Richardson, the secretary of the US Department of Health, Education, and Welfare, convened a group to recommend policies for the development of government databases that would protect the privacy of American citizens. The secretary's Advisory Committee of Automated Personal Data Systems, Records, Computers, and the Rights of Citizens produced a report for Congress that included the following "bill of rights" for the Information Age [73]:

Code of Fair Information Practices

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the

data for their intended use and must take precautions to prevent misuses of the data.

At about the same time that the Richardson Committee was established in the United States, similar efforts were under way in Europe. In fact, a year before the Richardson Committee issued the report containing the Code of Fair Information Practices, the Committee on Privacy in the United Kingdom released its own report containing many of the same principles. Sweden passed privacy laws consistent with fair information practices in 1973, and later that decade the Federal Republic of Germany and France followed suit [74].

6.7.2 Privacy Act of 1974

The Privacy Act of 1974 represents Congress's codification of the principles described in the Code of Fair Information Practices. While the Privacy Act does allow individuals in some cases to get access to federal files containing information about them, in other respects it has fallen short of the desires of privacy advocates. In particular, they say the Privacy Act has not been effective in reducing the flow of

personal information into governmental databases, preventing agencies from sharing information with each other, or preventing unauthorized access to the data. They claim agencies have been unresponsive to outside attempts to bring them into alignment with the provisions of the Privacy Act. The Privacy Act has the following principal limitations [75]:

1. *The Privacy Act applies only to government databases*.

   Far more information is held in private databases, which are excluded. This is an enormous loophole, because government agencies can purchase information from private organizations that have the data they want.

2. *The Privacy Act only covers records indexed by a personal identifier*.

   Records about individuals that are not indexed by name or another identifying number are excluded. For example, a former IRS agent tried to gain access to a file containing derogatory information about himself, but the judge ruled he did not have a right to see the file, since it was indexed under the name of another IRS employee.

3. *No one in the federal government is in charge of enforcing the provisions of the Privacy Act.*

   Federal agencies have taken it upon themselves to determine which databases they can exempt. The IRS has exempted its database containing the names of taxpayers it is investigating. The Department of Justice has announced that the FBI does not have to ensure the reliability of the data in its NCIC databases.

4. *The Privacy Act allows one agency to share records with another agency as long as they are for a "routine use."*

   Each agency is able to decide for itself what "routine use" means. The Department of Justice has encouraged agencies to define routine use as broadly as possible.

Although the Privacy Act applies only to government databases, Congress has also passed legislation regulating how some private institutions manage databases containing sensitive information about individuals, and these laws put into effect many of the principles of the Code of Fair Information Practices. In the remainder of this section, we survey some of the most influential of these laws.

6.7.3 Fair Credit Reporting Act

Credit bureaus and other consumer reporting agencies maintain information on your bill-paying record, whether you've been sued or arrested, and if you've filed for bankruptcy. They sell reports to other organizations that are trying to determine the credit-worthiness of consumers who are applying for credit, applying for a job, or trying to rent an apartment. The Fair Credit Reporting Act, passed in 1970 and revised in 1996, was designed to promote the accuracy and privacy of information used by credit bureaus and other consumer reporting agencies to produce consumer reports. It also ensures that negative information does not haunt a consumer for a lifetime.

The three major credit bureaus are Equifax, Experian, and TransUnion. According to the Fair Credit Reporting Act, these credit bureaus may keep negative information about a consumer for a maximum of seven years. There are several exceptions to this rule. The two most important are that information about criminal convictions may be kept indefinitely, and bankruptcy information may be held for 10 years.

6.7.4 Fair and Accurate Credit Transactions Act

The Fair and Accurate Credit Transactions Act of 2004 requires the three major credit bureaus to provide consumers a free copy of their credit report every 12 months. Consumers can use this opportunity to detect and correct errors in their credit reports. The bureaus do not issue the reports automatically; consumers must take the initiative and request them from AnnualCreditReport.com.

The law also has provisions to reduce identity theft. It requires the truncation of account numbers on credit card receipts, and it establishes the National Fraud Alert System. Victims of identity theft may put a fraud alert on their credit files, warning credit card issuers that they must take "reasonable steps" to verify the requester's identity before granting credit.

6.7.5 Financial Services Modernization Act

The Financial Services Modernization Act (also called the Gramm-Leach-Bliley Act of 1999) contains dozens of

provisions related to how financial institutions do business. One of the major provisions of the law allows the creation of "financial supermarkets" offering banking, insurance, and brokerage services.

The law also contains some privacy-related provisions. It requires financial institutions to disclose their privacy policies to their customers. When a customer establishes an account, and at least once per year thereafter, the institution must let the customer know the kinds of information it collects and how it uses that information. These notices must contain an opt-out clause that explains to customers how they can request that their confidential information not be revealed to other companies. The law requires financial institutions to develop policies that prevent unauthorized access to their customers' confidential information [76].

6.8 Data Mining by the Government

Data mining is the process of searching through one or more databases looking for patterns or relationships among the data. In this section we continue our coverage of the information-processing category of Solove's taxonomy by surveying a few well-known data-mining projects run by government agencies. We also consider harms that can result when data-mining algorithms create erroneous profiles of individuals.

6.8.1 Internal Revenue Service Audits

To identify taxpayers who have paid less in taxes than they owe, the Internal Revenue Service (IRS) uses computer-matching and data-mining strategies. First, it matches information on the tax form with information provided by employers and financial institutions. This is a straightforward way to detect unreported income.

Second, the IRS audits a couple of million tax returns every year. Its goal is to select the most promising returns—those containing errors resulting in underpayment of taxes. The IRS uses an algorithm called the discriminant function (DIF) to score every tax return. The DIF score is an indicator of how many irregularities there are on a tax form, compared to carefully constructed profiles of correct tax returns. About 60 percent of tax returns audited by the IRS are selected due to their high DIF scores.

6.8.2 Syndromic Surveillance Systems

Another application of data mining by the government is protecting society from imminent dangers.

A syndromic surveillance system is a computerized system that analyzes 911 calls, visits to the emergency room, school absenteeism, purchases of prescription drugs, and Internet searches to find patterns that might indicate the onset of an epidemic, an environmental problem leading to illnesses, or bioterrorism.

When the COVID-19 pandemic struck in the spring of 2020, people were encouraged to use hand sanitizers to help

prevent the spread of the virus. During this time a syndromic surveillance system in Arizona spotted a big increase in the number of methanol poisonings caused by people ingesting hand sanitizers. The Food and Drug Administration responded by recalling hand sanitizer products containing methanol [77].

6.8.3 Telecommunications Records Database

After September 11, 2001, several major telecommunications providers began turning over the phone call records of tens of millions of Americans to the National Security Agency, without a court order (see Section 6.6.5). The NSA was not monitoring or recording the actual conversations; instead, it was analyzing calling patterns in order to detect potential terrorist networks [78].

After *USA Today* revealed the existence of the database in May 2006, more than a dozen class-action lawsuits were filed against the telecommunications companies. In August 2006, a federal judge in Detroit ruled the program to be illegal and unconstitutional, violating several statutes as well as the First and Fourth Amendments to the US Constitution [79]. In July 2007, the US Court of Appeals for the Sixth Circuit

overturned the ruling on the grounds that the plaintiffs did not have standing to bring the suit forward. In other words, the plaintiffs had not produced any evidence that they personally were victims of the program.

6.8.4 Potential Harms of Profiling

Experts have begun to warn about the personal harms that can result when organizations pursue their objectives based on individual profiles they have constructed through data mining [80]. Sometimes those objectives are commercial. For example, as we saw in Chapter 5, Target used data mining to predict which of its customers were pregnant, so that they could use direct mail offers to get these customers into the habit of purchasing a wide variety of items at Target stores. In at least one case, Target sent advertisements for maternity clothing and nursery furniture to a teenage girl before she had told her father she was pregnant [81].

In other situations the objectives are much more serious. A government agency charged with protecting national security is responsible for preventing harm to the nation, and its employees are strongly motivated to take action before—not after—an attack. What happens if a learning algorithm

employed by a law enforcement agency mines a massive amount of data and constructs an erroneous profile of an individual, characterizing them as a potential terrorist? The amount of data being searched could be so massive, and the algorithms manipulating the data so complicated, that it might be impossible for any human being to explain why the algorithm has profiled a particular individual as a potential terrorist. How are innocent people who are identified on "terrorist watch lists" able to clear their names in this situation?

For example, there are now more than 1.5 million names on the US government's terrorist watch list, officially known as the Terrorist Screening Database [82]. Tens of thousands of these names somehow make their way to the government's "no-fly" list. Many people with common names (including the late Senator Edward Kennedy and the author of this book) have encountered problems boarding commercial flights because their names appeared on the "no-fly" list [83].

6.9 National Identification Card

A great deal can be learned about an individual when information collected at different places and times is combined. In order to combine information from two records, the records must share a common key. A name cannot be used as a common key, because more than one person can have the same name, but if every individual had a unique identification number and that identification number appeared in every database record referring to that individual, then all of these records could theoretically be combined into a massive "electronic dossier" documenting that person's life. In this section we survey the debate around the establishment of a national identification card in the United States.

6.9.1 History and Role of the Social Security Number

The Social Security Act of 1935 established two social insurance programs in the United States: a federal system of

old-age benefits to retired persons, and a federal-state system of unemployment insurance. Before the system could be implemented, employers and workers needed to become registered. The Social Security Board contracted with the US Postal Service to distribute applications for Social Security cards. The post office collected the forms, typed the Social Security cards, and returned them to the applicants. In this way over 35 million Social Security cards were issued in 1936–1937 [84].

The US government initially stated that Social Security numbers (SSNs) would be used solely by the Social Security Administration and not as a national identification card. In fact, from 1946 to 1972, the Social Security Administration put the following legend on the bottom of the cards it issued: "FOR SOCIAL SECURITY PURPOSES—NOT FOR IDENTIFICATION." However, use of the SSN has gradually increased. President Roosevelt ordered, in 1943, that federal agencies use SSNs as identifiers in new federal databases. In 1961 the Internal Revenue Service began using the SSN as the taxpayer identification number. Because banks report interest to the IRS, people must provide their SSN when they open a bank account. The SSN is typically requested on applications for credit cards. Motor vehicle departments and some other state agencies received permission to use SSNs as

identification numbers in 1976. The IRS now requires parents to provide the SSNs of their children over one year old on income-tax forms in order to claim them as dependents. For this reason, children now get SSNs soon after they are born. Many private organizations ask people to provide SSNs for identification. The SSN has become a de facto national identification number in the United States.

Unfortunately, the SSN has serious defects that make it a poor identification number. The first problem with SSNs is that they are not unique. When Social Security cards were first issued by post offices, different post offices accidentally assigned the same SSN to different people. In 1938 wallet manufacturer E. H. Ferree included sample Social Security cards in one of its products. More than 40,000 people purchasing the wallets from Woolworth stores thought the cards were real and used the sample card's number as their SSN [85].

A second defect of SSNs is that they are rarely checked. Millions of Social Security cards have been issued to applicants without verifying that the information provided by the applicants is correct. Many, if not most, organizations asking for SSNs do not actually require the applicant to show a card, making it easy for criminals to supply fake SSNs.

A third defect of SSNs is that they have no error-detecting capability, such as a check digit at the end of the number. A check digit enables computer systems to detect common data-entry errors, such as getting one digit wrong or transposing two adjacent digits. If someone makes one of these mistakes, the data-entry program can detect the error and ask the person to retype the number. In the case of SSNs, if a person accidentally types in the wrong number, there is a high likelihood that it is a valid SSN (albeit one assigned to a different person). Hence it is easy to contaminate databases with records containing incorrect SSNs [86]. Similarly, without check digits or another error-detection mechanism, there is no simple way for a system to catch people who are simply making up a phony SSN.

6.9.2 Debate over a National ID Card

The events of September 11, 2001, resurrected the debate over the introduction of a national identification card for Americans.

Proponents of a national identification card point out numerous benefits to its adoption:

1. *A national identification card would be more reliable than existing forms of identification.*

   Social Security cards and driver's licenses are too easy to forge. A modern card could incorporate a photograph as well as a thumbprint or other biometric data.

2. *A national identification card could reduce illegal immigration.*

   Requiring employers to check a tamper-proof, forgery-proof national identification card would prevent illegal immigrants from working in the United States. If illegal immigrants couldn't get work, they wouldn't enter the United States in the first place.

3. *A national identification card would reduce crime.*

   Currently, it's too easy for criminals to mask their true identity. A tamper-proof national identification card would allow police to positively identify the people they apprehend.

4. *National identification cards do not undermine democracy.*

Many democratic countries already use national ID cards, including Belgium, France, Germany, Greece, Luxembourg, Portugal, and Spain.

Opponents of a national identification card suggest these harms may result from its adoption:

1. *A national identification card does not guarantee that the apparent identity of an individual is that person's actual identity*.

   Driver's licenses and passports are supposed to be unique identifiers, but there are many criminals who produce fake driver's licenses and passports. Even a hard-to-forge identification card system may be compromised by insiders. For example, a ring of motor vehicle department employees in Virginia was caught selling fake driver's licenses [87].

2. *It is impossible to create a biometric-based national identification card that is 100 percent accurate*.

   All known systems suffer from false positives (erroneously reporting that the person does not match the ID) and false negatives (failing to report that the person and ID do not match). Biometric-based systems

may still be beaten by determined, technology-savvy criminals [87].

3. *There is no evidence that the institution of a national ID card would lead to a reduction in crime*.

   In fact, the principal problem faced by police is not the inability to make positive identifications of suspects but the inability to obtain evidence needed for a successful prosecution.

4. *A national identification card makes it simpler for government agencies to perform data mining on the activities of its citizens*.

   According to Peter Neumann and Lauren Weinstein, "The opportunities for overzealous surveillance and serious privacy abuses are almost limitless, as are opportunities for masquerading, identity theft, and draconian social engineering on a grand scale. . . . The road to an Orwellian police state of universal tracking, but actually *reduced* security, could well be paved with hundreds of millions of such [national identification] cards" [87].

5. *While most people may feel they have nothing to fear from a national identification card system since they are law-abiding citizens, even law-abiding people are*

> *subject to fraud and the indiscretions and errors of others*.
>
> Suppose a teacher, a doctor, or someone else in a position of authority creates a file about an individual that contains misleading or erroneous information. Files created by people in positions of authority can be difficult to remove [88].

In a society with decentralized record keeping, old school or medical records are less likely to be accessed so that the harm caused by inaccurate records is reduced. However, if all records are centralized around national identification numbers, files containing inaccurate or misleading information could haunt individuals for the rest of their lives.

6.9.3 The REAL ID Act

In May 2005, President George W. Bush signed the REAL ID Act, which is significantly changing driver's licenses in the United States. The motivation for passing the REAL ID Act was to make the driver's license a more reliable form of identification. Critics, however, say the act is creating a de facto national ID card in the United States.

The REAL ID Act requires that every state issue new driver's licenses. These licenses will be needed in order to open a bank account, fly on a commercial airplane, enter a federal building, or receive a government service, such as a Social Security check. The law makes it more difficult for impostors to get driver's licenses because it requires applicants to supply four different kinds of documentation, which is verified by state employees using federal databases. Because the new driver's license contains a biometric identifier, it is supposed to be a stronger credential than previous licenses [89].

Although each state is responsible for issuing new driver's licenses to its citizens, these licenses must meet federal standards. The license must include the person's full legal name, date of birth, gender, driver's license number, digital photograph, legal address, and signature. All data on the license must be in machine-readable form. The license must have physical security features designed to prevent tampering, counterfeiting, or duplication [90].

Supporters of the measure say making the driver's license a more reliable identifier will have numerous benefits. Law enforcement is easier when police can be more certain that a driver's license correctly identifies the individual carrying it. Society is better off when parents ducking child support and

criminals on the run cannot change their identities by crossing a state border and getting a new driver's license under a different name [**91**].

Some critics fear having machine-readable information on driver's licenses will aggravate problems with identity theft. Each state is required to share all driver's license information with every other state and with the federal government. American Civil Liberties Union lawyer Timothy Sparapani said, "We will have all this information in one electronic format, in one linked file, and we're giving access to tens of thousands of state DMV employees and federal agents" [**92**].

Proponents of the bill say such fears are unjustified. They suggest that the personal information available on the new driver's license is relatively insignificant compared to all the other personal information circulating around cyberspace [**91**].

The Department of Homeland Security repeatedly pushed back the deadline for implementing the new driver's license because of significant opposition in the states. Legislatures in about half the states passed laws or resolutions opposing the REAL ID Act, and many states passed laws prohibiting the

expenditure of state funds to implement the requirements of the REAL ID Act.

However, most states have now taken steps to come into compliance with the REAL ID Act to ensure their citizens will not face air travel restrictions when the Department of Homeland Security begins to require approved identification cards for commercial flights. The remaining states and US territories have been granted extensions by the Secretary of Homeland Security. Travelers 18 years of age and older will need REAL ID-compliant driver's licenses or ID cards by May 7, 2025, in order to use them as identification for domestic airline flights [**93**].

6.10 Information Dissemination

We now consider the information dissemination category of Solove's taxonomy. After we survey three federal laws that restrict the dissemination of personal information that organizations have collected, we discuss the Freedom of Information Act, designed to promote open government by allowing news organizations and private citizens to access records maintained by federal agencies. We explore how information collected by the government for one purpose—collecting tolls—is being used as evidence of people's whereabouts in both criminal and civil cases. Finally, we summarize an important US Supreme Court decision limiting police access to cell phone records.

6.10.1 Family Education Rights and Privacy Act

The Family Education Rights and Privacy Act (FERPA) provides students 18 years of age and older the right to review their educational records and to request changes to

records that contain erroneous information. Students also have the right to prevent information in these records from being released without their permission, except under certain circumstances. For students under the age of 18, these rights are held by their parents or guardians. FERPA applies to all educational institutions that receive funds from the US Department of Education.

6.10.2 Video Privacy Protection Act

In 1988 President Ronald Reagan nominated Judge Robert Bork to the US Supreme Court (Figure 6.5). Bork was a noted conservative, and his nomination was controversial. A Washington, DC, video store provided a list of Bork's video rental records to a reporter for the *Washington City Paper*, which published the list. While the intention of the paper was most likely to embarrass Bork, it also had the effect of prompting Congress to pass the Video Privacy Protection Act of 1988. According to this law, video providers (including providers of online videos) cannot disclose rental records without the written consent of the customer. In addition, organizations must destroy personally identifiable information about rentals within a year of the date when this

information is no longer needed for the purpose for which it was collected.

Figure 6.5

Judge Robert Bork, a nominee to the US Supreme Court, had to endure the publication of his video rental records by the *Washington City Paper*. (Charles Tasnadi/AP Images)

)

6.10.3 Health Insurance Portability and Accountability Act

As part of the Health Insurance Portability and Accountability Act of 1996, Congress directed the Department of Health and Human Services (HHS) to come up with guidelines for protecting the privacy of patients. These guidelines went into effect in April 2003. They limit

how doctors, hospitals, pharmacies, and insurance companies can use medical information collected from patients.

The regulations attempt to limit the exchange of information among health care providers to that information necessary to care for the patient. They forbid health care providers from releasing information to life insurance companies, banks, or other businesses without specific signed authorization from the person being treated. Health care providers must provide their patients with a notice describing how they use the information they gather. Patients have the right to see their medical records and to request corrections to errors they find in those records [94].

6.10.4 Freedom of Information Act

The Freedom of Information Act is a law designed to ensure that the public has access to US government records. Signed into law by President Johnson in 1966, it applies only to the executive branch of the federal government, not the legislative or judicial branches. The act carries a presumption that the government will release the requested records. If an

agency does not disclose records, it must explain why the information is being withheld.

There are nine exemptions in the Freedom of Information Act, spelling out those situations in which the government may legitimately withhold information. For example, a document may be withheld if it has been classified as secret for national defense or foreign policy reasons. The government may withhold the release of documents containing trade secrets or confidential commercial or financial information. Another exemption deals with documents related to law enforcement investigations.

6.10.5 Tollbooth Records Used in Court

E- ZPass is an automatic toll collection system used on most toll roads, bridges, and tunnels in the Midwest and Eastern United States. Drivers who have installed an E-ZPass tag (an RFID transponder) in their vehicles are able to pass through tollbooths without stopping to pay an attendant. Instead, an E-ZPass reader installed in the automated toll lane gets information from the tags of the cars that pass through and deducts the appropriate toll from each driver's account.

The New York State Department of Transportation (NYSDOT) has installed tag readers at locations other than tollbooths in order to track the progress of individual vehicles. In this way the system can provide helpful information to other drivers by displaying on electronic signs above the turnpike the estimated time to reach popular destinations. According to the NYSDOT, the system encrypts information from individual tags, deletes the information as soon as the vehicle passes the last reader, and never makes information about individual cars available to the department [**95**].

However, states do maintain records of when cars pass through tollbooths, and most of the states in the E-ZPass network provide information in response to court orders in criminal and civil cases. A well-known example is the case of Melanie McGuire, a New Jersey nurse suspected of murdering her husband and throwing his dismembered corpse into Chesapeake Bay. To help prove their case against McGuire, prosecutors used E-ZPass records to reconstruct her movements. E-ZPass records are also playing a role in divorce cases by providing evidence of infidelity [**96**].

6.10.6 *Carpenter v. United States*

In 2010–11 a series of nine armed robberies occurred at Radio Shack and T-Mobile stores in the Detroit area. In each case the robbers made off with sacks of cell phones. The police arrested four suspects in 2011. One of them confessed to the robberies, named his accomplices, and provided the FBI with the cell phone numbers of some of them [97].

Based on this information, the prosecutors sought court orders under the Stored Communications Act to obtain the cell phone records of Timothy Carpenter. The Stored Communications Act simply requires prosecutors to show that it is reasonable to believe the requested information is relevant to their investigation. That is an easier standard to meet than the demonstration of probable cause needed to get a search warrant. Federal magistrate judges approved the orders, and two wireless providers supplied 127 days of cell phone location records for Carpenter: 12,898 location points in all, averaging 101 data points per day [97].

Prosecutors charged Carpenter with "six counts of robbery and six counts of carrying a firearm during a federal crime of

violence" [97]. Carpenter's lawyer moved to suppress the evidence provided by the wireless carriers, arguing that the government's seizure of these records without a search warrant violated the Fourth Amendment to the US Constitution. The District Court denied the motion because of the third-party doctrine, which holds that people should not expect that information voluntarily given to third parties will be kept private. In this case, the wireless carriers were the third parties maintaining the location information from Carpenter's cell phones. During the trial, witnesses testified that Carpenter was the mastermind behind the robberies: planning them, supplying the guns, and serving as the lookout [98]. Prosecutors used the location information obtained by the wireless carriers to provide additional evidence that placed Carpenter at the scene of four of the robberies. Carpenter was found guilty on nearly all counts and was sentenced to more than 100 years in prison [97].

Carpenter's case went all the way to the US Supreme Court, which in June 2018 ruled 5–4 that the prosecutors had erred in "mechanically applying the third-party doctrine to this case" [97]. According to the majority opinion, written by Chief Justice Roberts, "Cell phone location information is not truly 'shared' as the term is normally understood" [97]. Therefore, the prosecutors violated the Fourth Amendment

when they seized Carpenter's cell phone records without a search warrant. The opinion noted wireless carriers are continually logging location information for all 400 million cell phones in the United States, not just those belonging to suspects in criminal investigations. "[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]. The location information obtained from Carpenter's wireless carriers was the product of a search" [97].

6.11 Invasion

Earlier in Chapter 5 we described privacy as a "zone of inaccessibility." People have information privacy to the extent that they have some control over who has access to their personal information. In quite a few modern situations, people may have very little control; they must cede access to their personal information if they wish to use the service provided. If the loss of control is accompanied by a loss of tranquility or interferes with someone's freedom of decision making, that is a privacy invasion, according to Solove. We begin this section by giving two examples of government actions to prevent invasion and then move on to survey two government actions that can be seen as invasive.

6.11.1 Telemarketing

After being sworn in as chairman of the Federal Trade Commission (FTC) in 2001, Timothy Muris looked for an action that the FTC could take to protect the privacy of Americans. It did not take long for the FTC to focus on telemarketing. A large segment of the American population views dinnertime phone calls from telemarketers as an annoying invasion of privacy. In fact, Harris Interactive

concluded that telemarketing is the reason why the number of Americans who feel it is "extremely important" not to be disturbed at home rose from 49 percent in 1994 to 62 percent in 2003 [**99**]. Responding to this desire for greater privacy, the FTC created the National Do Not Call Registry (www.donotcall.gov), a free service that allows people who do not wish to receive telemarketing calls to register their phone numbers. The public reacted enthusiastically to the availability of the Do Not Call Registry by registering more than 50 million phone numbers before it even took effect in October 2003 [**100, 101**].

The Do Not Call Registry has not eliminated 100 percent of unwanted solicitations. The regulations exempt political organizations, charities, and organizations conducting telephone surveys. Even if your phone number has been registered, you may still receive phone calls from companies with which you have done business in the past 18 months. The creation of the registry is a good example of how privacy is seen as a prudential right: the benefit of shielding people from telemarketers is judged to be greater than the harm caused by putting limits on telephone advertising.

6.11.2 Loud Television Commercials

Television watchers complained to the Federal Communications Commission (FCC) about loud commercials for fifty years. The Commercial Advertisement Loudness Mitigation Act (CALM Act), signed into law by President Barack Obama in December 2010, required the Federal Communications Commission to ensure that television commercials are played at the same volume as the programs they are interrupting.

6.11.3 Requiring Identification for Pseudoephedrine Purchases

In an effort to curb the illegal production of methamphetamine ("meth"), federal and state governments have passed laws limiting access to products containing pseudoephedrine, which is used in the manufacture of methamphetamine. The Combat Methamphetamine

Epidemic Act limits the quantity of pseudoephedrine that an individual can purchase in a month. Whether the laws have been effective is a matter of debate. In most states, original Sudafed is still sold behind the counter to adults, but they must show an identification card and fill out a sales log with their name, address, and signature. Two states, Oregon and Mississippi, require a prescription to acquire a product containing pseudoephedrine. In several well publicized cases, grandparents purchasing cold medicine for members of their families have been arrested by police for exceeding limits set on pseudoephedrine purchases [**102**].

6.11.4 Advanced Imaging Technology Scanners

In an effort to provide enhanced passenger security at airports, the Transportation Security Administration began deploying advanced imaging technology (AIT) scanners in 2007. Some AIT scanners use backscatter X-rays to produce a detailed image of the passenger's body, and other scanners use millimeter waves. The TSA began testing AIT systems at Phoenix's Sky Harbor International Airport in 2007 [**103**]. When the first AIT system was deployed, passengers who failed the primary security screening could choose between

the X-ray scan and a traditional pat-down search. In June 2011, the Transportation Security Administration announced that it had already deployed 500 AIT units and would deploy an additional 500 units, enabling it to use this technology to screen 60 percent of all airline passengers in the United States [**104**]. Even as it was busily deploying systems, the TSA was battling critics.

Some people were offended at the images produced by AIT scanners, which reveal "all anatomical features" (Figure 6.6) [**105**]. Lawyers for the American Civil Liberties Union called the AIT scan a "virtual strip-search" [**106**]. In July 2010, the Electronic Privacy Information Center filed a lawsuit to suspend the deployment of AIT systems, pending further review. EPIC called the program "unlawful, invasive, and ineffective," arguing that it violated the Privacy Act, the Religious Freedom Restoration Act, and the Fourth Amendment to the US Constitution [**107**].

Figure 6.6

In February 2011, the Transportation Security Administration announced that it was about to begin testing new software on its advanced imaging technology machines that would eliminate passenger-specific images. TSA Administrator John Pistole said that the new system “auto-detects potential threat items and indicates their location on a generic outline of a person” [**108**]. The tests were successful, and in January 2013 the TSA announced that all body scanners producing passenger-specific images would be removed from airport checkpoints by June 2013 [**109**].

Summary

It's only natural that people want government to leave them alone, but they also expect government to keep them safe and secure through effective policing and a strong national defense. Frequently, the constitutional guarantees in the Bill of Rights come into conflict with the desires of law enforcement agencies to gather information that can help them apprehend criminals. Through legislation, administrative policies, and court decisions, the three branches of the US government have been engaged in an attempt to find the right balance between competing concerns.

In this chapter we looked at the role that federal, state, and local governments have played in protecting and eroding the information privacy of individual citizens. We organized our presentation using the taxonomy of privacy proposed by Daniel Solove, which divides the field into four categories: information collection, information processing, information dissemination, and invasion. We reviewed legislation and administrative policies that protect the information privacy of

individuals by restricting how organizations can collect, process, and disseminate information as well as limit the extent to which they can intrude into people's daily lives. We also looked at ways in which governments have promoted public safety and security by collecting, processing, and disseminating personal information and intruding into people's lives.

We surveyed many governmental activities related to information collection. The federal government maintains extensive databases containing a vast amount of information about individual Americans, and from time to time information in these databases has been misused. The government also collects information through overt and covert surveillance.

After the terrorist attacks of September 11, 2001, concerns about individual privacy took a backseat to concerns about national security, and significant changes occurred in the government's activities related to information collection, information processing, and invasion. The Patriot Act amended many laws and enhanced the ability of law enforcement agencies to gather information about suspected terrorists and criminals. The National Security Agency illegally acquired records of domestic phone calls from

telecommunications companies and performed data mining in an attempt to find calling patterns indicating the presence of terrorist networks. The Transportation Security Administration installed invasive advanced imaging technology scanners at airport security checkpoints. As the horizon of the September 11 attacks has receded, the public's discomfort with many of these operations has increased, and some of them have been scaled back.

The Social Security number is an important identifier in the United States, but it has many flaws. The US Congress passed the REAL ID Act that created a new federal standard for driver's licenses. Once every state comes into compliance, the driver's license will probably become the most trusted form of identification in the United States, a de facto national identification card.

Further Reading, Listening, and Viewing

Julia Angwin. “One of the Last Bastions of Digital Privacy Is Under Threat.” *New York Times*, June 13, 2023. https://www.nytimes.com/2023/06/13/opinion/encryption-messaging-privacy-signal-whatsapp.html.

James Bamford. “The Black Box.” *Wired*, April 2012.

Dan Boylan. “Is the Notion of Privacy Outdated?” *Insights on PBS Hawaii*, July 11, 2013. 56:49. video.pbs.org.

Patrick A. Hafner. “Naked Citizens.” *Journeyman Pictures*, May 2013. 32:41.topdocumentary films.com/naked-citizens.

Mikko Hypponen. “How the NSA Betrayed the World’s Trust—Time to Act.” *TEDxBrussels*, October 2013. 19:14. www.ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_

Paul Mozur, Muyi Xiao, and John Liu. “‘An Invisible Cage’: How China Is Policing the Future.” *New York*

Times, June 25, 2022. https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html.

Emily Mullin. "A Rape Survivor Gave Police Her DNA. They Linked Her to Another Crime." *WIRED*, February 24, 2022. https://www.wired.com/story/a-rape-survivor-gave-police-her-dna-they-linked-her-to-another-crime.

Emily Mullin. "Police Used a Baby's DNA to Investigate Its Father for a Crime." *WIRED*, August 15, 2022. https://www.wired.com/story/police-used-a-babys-dna-to-investigate-its-father-for-a-crime/.

Paul Ohm. "Legalese: The 'Third Party Doctrine' and Carpenter v. United States." *Georgetown Law*, June 25, 2018. 2:19. www.youtube.com/watch?v=2ZH9Bd-pCrg.

Daniel J. Solove. "Why Privacy Matters Even If You Have 'Nothing to Hide.'" *Chronicle of Higher Education*, May 15, 2011.

Hari Sreenivasan. "Rise of Domestic Drones Draws Questions About Privacy." *PBS News-Hour*, April 18, 2013. 7:30. video.pbs.org.

Margaret Warner. “Surveillance Court Can’t Stop NSA from Violating Privacy.” *PBS News-Hour*, August 16, 2013. 6:33. video.pbs.org.

Review Questions

1. Determine the relationship between the categories of Daniel Solove's taxonomy of privacy and the following definitions of privacy proposed by other authors:
    - Privacy is the right to be left alone. (Warren and Brandeis)
    - Privacy is control over who knows what about us. (Rachels)
    - Privacy is the appropriate flow of personal information. (Nissenbaum)
2. How did the position of the US Supreme Court toward wiretapping evolve over time? Cite the key cases.
3. Give three examples of legislation passed by the US Congress designed to protect the privacy of residents of the United States.
4. Give three examples of US government agencies successfully achieving their ends using data legally obtained from residents of the United States.

5. Give three examples of US government agencies illegally collecting or disseminating information about residents of the United States in order to achieve their ends.

6. What are telephony metadata? Briefly summarize the history of the controversy surrounding the collection of telephony metadata by the National Security Agency after 9/11.

7. Describe similarities and differences between these covert surveillance programs of the US government: Operation Shamrock, Carnivore, PRISM, NSA wiretapping after 9/11, NSA collection of telephony metadata after 9/11.

8. What are the implications of the Stored Communications Act for all those who let an Internet service provider handle their email?

9. Why has the expanded use of National Security Letters raised privacy concerns?

10. Briefly summarize in your own words the five tenets of the Code of Fair Information Practices.

11. Robert Bellair has said, “The Privacy Act, it turns out, is no protection at all. You can drive a truck through

the Privacy Act" [75, p. 212]. Why do Bellair and other privacy advocates feel the Privacy Act of 1974 is a weak piece of legislation?

12. What actions has the US Congress taken to help ensure people aren't disadvantaged by poor credit ratings because of erroneous or obsolete information?

13. Give three examples of how information collected by a government for one purpose has been used for an entirely different purpose.

14. What are the problems with using the Social Security number as an identification number?

15. Give two arguments in favor of a national identification card for the United States. Give two arguments against creating a national identification card.

16. For each category in Daniel Solove's taxonomy of privacy, give one example of a law passed by the US Congress protecting individual privacy of that type.

Discussion Questions

17. Do you think local governments should increase the use of video cameras at intersections to help ensure drivers who run red lights are identified and ticketed?

18. Florida, Missouri, Ohio, and Oklahoma have passed laws that require lifetime monitoring of some convicted sex offenders after they have been released from prison. The offenders must wear electronic ankle bracelets and stay close to small GPS transmitters, which can be carried on a belt or in a purse. Computers monitor the GPS signals and alert law enforcement officials if the offenders venture too close to a school or other off-limits area. Police interested in the whereabouts of a monitored person can see their location, traveling direction, and speed plotted on a map [**110**].

    Do these laws represent an unacceptable weakening of personal privacy, or are they sensible public safety measures? Should they be repealed? Should people

convicted of other crimes also be monitored for life? Would there be less crime if everyone in society were monitored?

19. Think about what you do when you get up in the morning. How would you act differently if you knew you were being watched? Would you feel uncomfortable? Do you think you would get used to being watched?

20. Discuss the following responses to the revelation that telecommunications companies provided domestic phone call records to the National Security Agency [**111**].

    President George Bush: "Al-Qaeda is our enemy, and we want to know their plans."

    Senator Patrick Leahy of Vermont: "Are you telling me tens of millions of Americans are involved with al-Qaeda?"

    Senator Jon Kyl of Arizona: "We are in a war, and we have got to collect intelligence on the enemy."

    Senator Chuck Grassley of Iowa: "Why are the telephone companies not protecting their customers? They have a social responsibility to

people who do business with them to protect our privacy as long as there isn't some suspicion that we're a terrorist or a criminal or something."

21. When asked about Google releasing personal information to law enforcement agencies, Google's CEO Eric Schmidt told CNBC: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" [**58**]. Discuss Mr. Schmidt's perspective.

22. Was the US government's $2 million settlement with Brandon Mayfield reasonable and just?

23. In order to combat the counterfeiting of currency, the US Secret Service convinced several color laser printer manufacturers to add a secret code to every printed page. The code is invisible to the human eye but can be seen under a microscope. When decrypted, it reveals the serial number of the printer and the time and date the page was printed [**112**].

    By agreeing to secretly insert the codes, did the printer manufacturers violate the privacy rights of their customers?

24. What special responsibilities do computer professionals have with respect to understanding and protecting the privacy rights of their fellow citizens?

In-Class Exercises

25. The Code of Fair Information Practices applies only to government databases. Debate the advantages and disadvantages of extending the Code of Fair Information Practices to private databases managed by corporations.

26. A database containing the DNA information of every citizen of a country could be a valuable resource to medical researchers. It could also help police solve crimes. Debate the following proposition: It would be in the best interests of society if the government constructed a DNA database of every resident and made the database available to medical researchers and law enforcement agencies.

27. Debate the proposition that every adult resident of the United States ought to carry a national identification card.

28. Debate the following proposition: By creating the Threat and Local Observation Notices (TALON) database, which enabled citizens to report on each

other's activities, the US government effectively reduced freedom of speech.

References

[1] Ben Popper. “How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars.” *The Verge* (Web site), December 10, 2014. https://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

[2] “Stop the Government’s Massive Privacy Invasion.” American Civil Liberties Union (Web site). Accessed July 13, 2023. https://action.aclu.org/send-message/stop-governments-massive-privacy- invasion.

[3] Bryon Tau and Michelle Hackman. “Federal Agencies Use Cellphone Location Data for Immigration Enforcement; Commercial Database That Maps Movements of Millions of Cellphones Is Deployed by Immigration and Border Authorities.” *Wall Street Journal*, February 7, 2020.

[4] Jason Kelley and Matthew Guariglia. “Ring Reveals They Give Videos to Police Without User Consent or a Warrant.” Electronic Frontier Foundation (Web site), July 15, 2022. https://www.eff.org/deeplinks/2022/07/ring-reveals-

they-give-videos- police-without-user-consent-or-warrant.

[5] Daniel J. Solove. *Understanding Privacy*. Harvard University Press, Cambridge, MA, 2008.

[6] Natasha Singer. "Epic Games to Pay $520 Million Over Children's Privacy and Trickery Charges." *New York Times*, December 19, 2022. https://www.nytimes.com/2022/12/19/business/ftc-epic-games-settlement.html.

[7] "GINA: The Genetic Information Nondiscrimination Act of 2008: Information for Researchers and Health Care Professionals." Department of Health and Human Services, USA, April 6, 2009. www.genome.gov.

[8] Stephanie L. Hitt. "NCIC 2000." *FBI Law Enforcement Bulletin,* 69(7): 12–15, July 2000. Accessed July 14, 2023. le.fbi.gov/informational-tools/ncic.

[9] Federal Bureau of Investigation. National Crime Information Center (Web page).

[10] "National Data Exchange (N-DEx)." Federal Bureau of Investigation (Web site). Accessed July 14, 2023.

https://le.fbi.gov/informational-tools/national-data-exchange-n-dex.

[11] Kasey Wertheim. “Recent Improvements to the FBI’s National Data Exchange (N-DEx).” *Police Chief*. Accessed July 14, 2023. https://www.policechiefmagazine.org/recent-improvements-to-the-fbis-ndex/.

[12] John T. Eberth. “Nation’s First Surveillance Cameras Were Installed in Olean.” *Olean Times Herald*, October 5, 2008. www.oleantimesherald.com.

[13] Jurgita Lapienyte. “This Is the Most Heavily Surveilled City in the US: 50 CCTV Cameras per 1,000 Citizens.” *Cybernews* (Web site), September 28, 2021. https://cybernews.com/editorial/this-is-the-most-heavily-surveilled- city-in-the-us-50-cctv-cameras-per-1000-citizens/.

[14] Chris Dolmetsch. “Cameras to Catch Terrorists Triple in New York with Bomb Plots.” *Bloomberg*, November 13, 2010. www.bloomberg.com.

[15] Jamie Roth. “Bloomberg in London to Study Security System.” *WABC Local News*, May 11, 2010. abclocal.go.com/wabc/.

[16] Jennifer Lee. “Study Questions Whether Cameras Cut Crime.” *New York Times*, March 3, 2009.

[17] M. Angela Sasse. “Privacy and Security: Not Seeing the Crime for the Cameras?” *Communications of the ACM*, 53(2): 22–25, February 2010.

[18] Patrick Grother, Mei Ngan, and Kayee Hanaoka. “Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects.” National Institute of Standards and Technology, NISTIR 8280, December 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[19] Clare Garvie. “A Forensic without the Science: Face Recognition in U.S. Criminal Investigations.” *Center on Privacy & Technology at Georgetown Law*, December 6, 2022. https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Cri

[20] Paresh Dave. “U.S. Cities Are Backing Off Banning Facial Recognition as Crime Rises.” *Reuters*, May 12, 2022. https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/.

[21] James R. Healey, Greg Toppo, and Fred Meier. "You Can't Hide from Cops with License-Plate Scanners." *USA Today*, July 18, 2013. www.usatoday.com.

[22] Adam Goldman and Matt Apuzzo. "With Cameras, Informants, NYPD Eyed Mosques." Associated Press, February 23, 2012. www.ap.org.

[23] "Automated License Plate Readers—State Statutes Regulating Their Use." National Conference of State Legislatures, February 2, 2015. www.ncsl.org.

[24] Federal Aviation Administration. "Fact Sheet—Unmanned Aircraft Systems (UAS)" (press release). February 19, 2013. www.faa.gov.

[25] Maggie Clark. "States Seek Legal Limits on Domestic Drones." *Stateline*, February 22, 2013. www.pewstates.org.

[26] Monmouth University. "US Supports Some Domestic Drone Use" (press release). June 12, 2012.

[27] Maggie Clark. "Boston Bombings Show Future Use for Police Drones." *Stateline*, May 2, 2013. www.pewstates.org.

[28] Whitfield Diffie and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT

Press, Cambridge, MA, 1998.

[29] Priscilla M. Regan. *Legislating Privacy*. University of North Carolina Press, Chapel Hill, NC, 1995.

[30] Justice Brandeis, Dissenting. Supreme Court of the United States. Olmstead v. United States, 277 US 438 (1928).

[31] Supreme Court of the United States. Katz v. United States, 389 US 347 (1967).

[32] James Bamford. *The Puzzle Palace: A Report on America's Most Secret Agency*. Penguin Books, New York, NY, 1983.

[33] Heinz Tschabitscher. "How Carnivore Email Surveillance Worked." About.com. Accessed October 15, 2013. email.about.com.

[34] Holly E. Ventura, J. Mitchell Miller, and Mathieu Deflem. "Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power." *Critical Criminology,* 13(1): 55–70, January 2005.

[35] US District Court, Central District of California, Western Division. "In the Matter of the Application of the United States of America for an Order Authorizing

the Installation of a Pen Register and Trap and Trace Device." Criminal No. 99-2713M, February 4, 2000.

[36] Kevin Poulsen. "FBI Retires Its Carnivore." *SecurityFocus*, January 14, 2005. www.securityfocus.com.

[37] James Risen and Eric Lichtblau. "Bush Lets US Spy on Callers Without Courts." *New York Times*, December 16, 2005.

[38] Lisa Myers, Douglas Pasternak, Rich Gardella, and the NBC Investigative Unit. "Is the Pentagon Spying on Americans?" MSNBC.com, December 14, 2005.

[39] Samantha Henig. "Pentagon Surveillance of Student Groups Extended to Scrutinizing E-mail." *Chronicle of Higher Education*, 52(46): 18, July 21, 2006.

[40] "No Real Threat: The Pentagon's Secret Database on Peaceful Protest." American Civil Liberties Union, January 17, 2007. www.aclu.org.

[41] Siobhan Gorman. "Intelligence Policies Shift: Pentagon Spy Chief Rolling Back Some of Rumsfeld's Strategies." *Baltimore Sun*, May 26, 2007.

[42] Nate Anderson. "US to Shutter DoD TALON Database as It Works on Replacement." Ars Technica (Web site), August 21, 2007. www.arstechnica.com.

[43] Glenn Greenwald and Ewen MacAskill. "NSA Prism Program Taps In to User Data of Apple, Google and Others." *Guardian*, June 6, 2013.

[44] Orin S. Kerr. "The Case for the Third-Party Doctrine." *Michigan Law Review*, 107: 561–601, February 2009.

[45] David Kravets. "Yahoo, Feds Battle over E-mail Privacy." Threat Level: Privacy, Crime and Security Online, *Wired*, April 14, 2010. www.wired.com.

[46] Ryan Singel. "Google, Microsoft Push Feds to Fix Privacy Laws." Threat Level: Privacy, Crime and Security Online, *Wired*, March 30, 2010. www.wired.com.

[47] Nancy Gohring. "FCC Inflates CALEA." *Telephony,* 237(10): 8, September 6, 1999.

[48] Charlotte Twight. "Conning Congress." *Independent Review,* 6(2): 185, Fall 2001.

[49] Kirk Laughlin. "A Wounded CALEA Is Shuttled Back to the FCC." *America's Network,* 104(15): 22, October 1, 2000.

[50] "FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps." *Federal Communications Commission*, August 5, 2005. www.fcc.gov.

[51] "USA PATRIOT Act: Major Provisions of the 2001 Antiterrorism Law." *Congressional Digest,* 82(4): 110–112, April 2003.

[52] Pete Yost. "FBI Access to E-mail, Web Data Raises Privacy Fear." Associated Press, July 30, 2010. seattletimes.nwsource.com.

[53] "Annual Statistical Transparency Report: Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2021." Office of Civil Liberties, Privacy, and Transparency, Office of the Director of National Intelligence, United States of America, April 2022. https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_C

[54] American Civil Liberties Union. "With Help of ACLU, Connecticut Library Group Successfully Keeps Patron Records Private" (press release). June 26, 2006. www.aclu.org.

[55] "PATRIOT Act Fears Are Stifling Free Speech, ACLU Says in Challenge to Law." American Civil Liberties

Union, New York, NY, November 11, 2003. www.aclu.org.

[56] American Library Association. "Resolution on the USA PATRIOT Act and Related Measures That Infringe on the Rights of Library Users." 2003 ALA Midwinter Meeting, 2002–2003 CD #20.1, January 29, 2003. www.ala.org.

[57] Bill of Rights Defense Committee (Web site). Accessed September 2, 2011. www.bordc.org.

[58] Cade Metz. "Google Chief: Only Miscreants Worry About Net Privacy." *Register*, December 7, 2009. www.theregister.co.uk.

[59] Tom Ridge. "Using the PATRIOT Act to Fight Terrorism." *Congressional Digest*, 83(9): 266–268, November 2004.

[60] Ben Jacklet and Todd Murphy. "Now Free, Attorney Brandon Mayfield Turns Furious." *Washington Report on Middle East Affairs* 23(6), July/August 2004.

[61] Dan Eggen. "Flawed FBI Probe of Bombing Used a Search Warrant." *Washington Post*, April 7, 2005.

[62] Eric Lichtblau. “U.S. Will Pay $2 Million to Lawyer Wrongly Jailed.” *New York Times*, November 30, 2006. www.localnewsdaily.com.

[63] Andrew Murr, Michael Isikoff, Eric Pape, and Mike Elkin. “The Wrong Man.” *Newsweek* 143(23), June 7, 2004.

[64] Ron Wyden. “Wyden Warns of Potential Public Backlash from Allowing Secret Law.” YouTube(video), uploaded May 27, 2011. youtube.com/watch?v=vMAX_Frj8xM.

[65] Glenn Greenwald. “NSA Collecting Phone Records of Millions of Verizon Customers Daily.” *Guardian*, June 5, 2013.

[66] “White House Defends NSA Order to Verizon to Reveal Call Data.” UPI, June 6, 2013. www.upi.com.

[67] Charlie Savage and Edward Wyatt. “Verizon Case Offers Glimpse of Vast N.S.A. Surveillance.” *New York Times*, June 6, 2013.

[68] Dan Roberts and Spencer Ackerman. “Anger Swells After NSA Phone Records Court Order Revelations.” *Guardian*, June 6, 2013.

[69] Charlie Savage and Jonathan Weisman. “N.S.A. Collection of Bulk Call Data Is Ruled Illegal.” *New York Times*, May 7, 2015. www.nytimes.com.

[70] Jennifer Steinhauer and Jonathan Weisman. “U.S. Surveillance in Place Since 9/11 Is Sharply Limited.” *New York Times*, June 2, 2015. www.nytimes.com.

[71] Carl Kaysen. “Data Banks and Dossiers.” *Public Interest*, 7: 52–60, Spring 1967.

[72] G. Russell Pipe. “Privacy: Establishing Restrictions on Government Inquiry.” *American University Law Review*, 18: 516–551, 1969.

[73] US Department of Health, Education, and Welfare. “Code of Fair Information Practices.” Secretary’s Advisory Committee of Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, 1973.

[74] Robert Gellman. “Fair Information Practices: A Basic History.” July 15, 2011. bobgellman.com.

[75] William Petrocelli. *Low Profile: How to Avoid the Privacy Invaders*. McGraw-Hill, New York, NY, 1981.

[76] "Fact Sheet 24: Protecting Financial Privacy." Privacy Rights Clearinghouse, July 14, 2005. www.privacyrights.org.

[77] "Tracking Methanol Poisonings Associated with Recalled Hand Sanitizer Products in Arisona, July–October 2020." National Syndromic Surveillance Program (NSSP), Centers for Disease Control and Prevention, June 16, 2023. https://www.cdc.gov/nssp/success-stories/Tracking-Methanol- Poisonings.html.

[78] Leslie Cauley. "NSA Has Massive Database of Americans' Phone Calls." *USA Today*, May 11, 2006.

[79] Wayne Rash. "Federal Court Finds NSA Wiretaps Unconstitutional." *eWeek.com*, August 18, 2006. www.eweek.com.

[80] Kate Crawford and Jason Schultz. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms." *Boston College Law Review*, 55(1): 93–128, January 29, 2014. lawdigitalcommons.bc.edu.

[81] Kashmir Hill. "How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did." *Forbes*, February 16, 2012. www.forbes.com.

[82] Matthew Barakat. “Terrorist Database Continues to Grow at Rapid Rate.” Big Story (Web site), July 18, 2014. bigstory.ap.org.

[83] Jeremy Scahill and Ryan Devereaux. “The Secret Government Rulebook for Labeling You a Terrorist.” *Intercept*, July 23, 2014. firstlook.org.

[84] “A Brief History of Social Security.” Social Security Administration, USA, August 2000.

[85] “Social Security Cards Issued by Woolworth.” Social Security Administration, USA. Accessed October 15, 2013. www.ssa.gov/history/ssn/misused.html.

[86] “Extent of Social Security Number Discrepancies.” Office of Inspector General, Department of Health and Human Services, USA. OAI-06-89-01120, January 1990.

[87] Peter G. Neumann and Lauren Weinstein. “Risks of National Identity Cards.” *Communications of the ACM*, 44(12): 176, December 2001.

[88] Richard Turner. Letter to the Editor. *Times*, London, September 7, 2001.

[89] Declan McCullagh. “FAQ: How Real ID Will Affect You.” *New York Times*, May 6, 2005.

[90] "REAL ID Act of 2005 Driver's License Title Summary." Real Nightmare.org (Web site). Accessed October 15, 2013. www.realnightmare.org/images/File/NCSL_Summary_of_Real_

[91] Dennis Bailey. *The Open Society Paradox: Why the 21st Century Calls for More Openness—Not Less*, p. 42 Potomac Books, Washington, DC, 2004.

[92] Joseph Menn. "Federal ID Act May Be Flawed." *Los Angeles Times*, May 31, 2005.

[93] "Be Your REAL ID Self." Department of Homeland Security, United States of America. Accessed July 17, 2023. https://www.dhs.gov/real-id.

[94] "Protecting the Privacy of Patients' Health Information." Department of Health and Human Services, USA, April 14, 2003. www.hhs.gov/news.

[95] New York State Department of Transportation. "NYSDOT Announces Travel Time Signs in Staten Island" (press release). July 10, 2007. www.nysdot.gov.

[96] Chris Newmarker. "E-ZPass Records Out Cheaters in Divorce Court." Associated Press, August 10, 2007. www.msnbc.com.

[97] C. J. Roberts. Supreme Court of the United States. Carpenter v. United States, 16–402 (2018).

[98] Adam Liptak. “In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy.” *New York Times*, June 22, 2018.

[99] Humphrey Taylor. “Most People Are ‘Privacy Pragmatists’ Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits.” HarrisInteractive, Harris Poll #17, March 19, 2003.

[100] James Toedtman. “Court Unblocks Do Not Call Registry in Latest Ruling.” *Sun-Sentinel*, Fort Lauderdale, FL, October 8, 2003.

[101] Heather Fleming Phillips. “Consumers Can Thank Do-Not-Underestimate FTC Chairman for Do-Not-Call Peace.” *San Jose Mercury News*, January 2, 2004.

[102] Radley Balko. “As It Turns Out, Meth Laws Have Unintended Consequences.” *Washington Post*, October 14, 2014. www.washingtonpost.com.

[103] Ginger D. Richardson. “Revealing X-Ray Machine Set to Scan Sky Harbor Flyers.” *Arizona Republic*, February 23, 2007. www.azcentral.com/arizonarepublic.

[104] Statement of John S. Pistole, Administrator, Transportation Security Administration, Before the US House of Representatives. Committee on Homeland Security, Subcommittee on Transportation Security, June 2, 2011. www.tsa.gov.

[105] Melissa Cheung. "New Airport X-Ray Too Revealing?" *CBS News*, February 11, 2009. www.cbsnews.com.

[106] Paul Giblin and Eric Lipton. "New Airport X-Rays Scan Bodies, Not Just Bags." *New York Times*, February 24, 2007.

[107] "Whole Body Imaging Technology and Body Scanners ('Backscatter' X-Ray and Millimeter Wave Screening)." Electronic Privacy Information Center (Web site). Accessed July 9, 2011. epic.org/privacy/airtravel/backscatter/.

[108] Transportation Security Administration. "TSA Begins Testing New Advanced Imaging Technology Software" (press release). February 1, 2011.

[109] Mike M. Ahlers. "TSA Removing 'Virtual Strip Search' Body Scanners." *CNN*, January 18, 2013. www.cnn.com.

[110] David A. Lieb. "States Move on Sex Offender GPS Tracking." Associated Press, July 30, 2005.

[111] Susan Page. "NSA Secret Database Report Triggers Fierce Debate in Washington." *USA Today*, May 11, 2006.

[112] John P. Mello Jr. "Codes Make Printers Stool Pigeons." *E-Commerce Times*, October 18, 2005. www.ecommercetimes.com.

Chapter 7

Computer and Network Security

7.1 Introduction

DO YOU HAVE A HOME NETWORK? IF SO, THERE IS A MODEM THAT LINKS your network to the Internet and a wireless router that connects with your devices. Usually the two functions are combined into a single device. Have you changed the default administrator password on the router? If not, it may be compromised. More than 500,000 routers are infected with malware capable of stealing passwords and intercepting financial information [**1**].

Do you ever go to a coffee shop and use its open wireless network to surf the Web? That's risky behavior. Freely available software gives any nearby computer user the ability to break into the accounts of people accessing Web sites through password-free wireless networks.

In the movie *Live Free or Die Hard*, a terrorist organization hacks into a variety of computer and communication systems to seize control of traffic lights, natural gas pipelines, and electrical power grids. Are such episodes purely the stuff of Hollywood fiction, or could they really happen?

This chapter focuses on threats to computer and network security. Millions of people and most businesses rely upon

computers and the Internet to conduct their affairs, making the security of these systems an important issue. Without adequate security, computers are vulnerable to criminal enterprises that introduce malicious software to reap valuable financial information or extort payments from computer users. Computers can also be co-opted and used as weapons by governments seeking to further their political aims by sponsoring attacks on the cyber infrastructure of their enemies.

We begin our survey with examples of individuals using cunning or skill to gain unauthorized access to computer systems.

7.2 Hacking

In the 1983 movie *WarGames*, a teenager breaks into a military computer and nearly causes a nuclear Armageddon. After seeing the movie, a lot of teenagers were excited at the thought that they could prowl cyberspace with a home computer and a modem. A few of them became highly proficient at breaking into government and corporate computer networks. These actions helped establish the everyday meaning of the word "hacker."

Today's hackers are people who gain unauthorized access to computers and computer networks. An example of the modern use of this word is a story in the July 20, 2023, issue of the *New York Times*, which contains an obituary for Kevin Mitnick, "best known for an audacious hacking spree in the 1990s" [2].

7.2.1 How Hackers Get Passwords

Typically, you need a login name and password to access a computer system, but good hackers are adept at guessing

short or predictable passwords. In 2013 Ars Technica asked three hackers to attack a list of 16,000 hashed passwords. Using computers, the hackers generated candidate passwords from strings of characters, hashed the candidates, and then checked the hashes against the list, looking for matches. The least successful hacker spent one hour on the task and identified 62 percent of the passwords. The most successful hacker worked for 20 hours and identified 90 percent of the passwords, using a commodity PC equipped with an AMD Radeon 7970 graphics card [3].

Hackers employ brute-force methods to guess shorter passwords. Passwords are constructed from a set of 95 characters: 26 uppercase letters, 26 lowercase letters, 10 digits, and 33 symbols. That means there are 95 passwords of length 1, 95^2 passwords of length 2, 95^3 passwords of length 3, and so on. The total number of passwords up to length 6 is about 744 billion. That may seem like a lot of passwords to you, but a computer can try all of these combinations in just a few minutes.

Hackers use **dictionary attacks** to guess longer passwords. Armed with lists of words that commonly appear in passwords, they generate candidate passwords using a variety of strategies, such as combining words, inserting random

characters before or after the words, and replacing characters in words with random characters.

In the experiment conducted by Ars Technica, the hackers' dictionary attacks identified a surprising number of long passwords, including "Apr!l221973," "ilovetofunot," "BandGeek2014," "ilovemySister31," and "Philippians4:6-7" [3].

Sidebar: Responsible Computer Users Take Passwords Seriously

Here is a list of password dos and don'ts from security experts [3, 4, 5].

- **Do not use short passwords.** Modern computers can quickly crack short passwords. As a general rule, the longer a password is, the less likely it is to be guessed. Choose passwords with at least 11 characters.

- **Do not rely solely on words from the dictionary.** Again, such a password is too easy to crack. Make sure your passwords include numbers, as well as upper- and lowercase letters.

- **Do not rely on substituting numbers for letters** (e.g., replacing "E" with "3" and "A" with "4"). Password-cracking programs know these tricks.
- **Do not reuse passwords.** If accounts share passwords, as soon as one account is compromised, the other ones are, too. If you must write down your passwords on a piece of paper in order to remember them, that is safer than reusing passwords in today's environment where an online attack is a greater danger than someone rummaging through your desk. (Of course, you should put sensitive documents like password lists in a locked drawer.)
- **Give ridiculous answers to security questions.** That way they serve as a secondary password.

Example: What is your pet's name? Ford Fiesta.

- **Enable two-factor authentication if available.** When you log in from an unfamiliar computer, the system will send you a text message with a confirmation code.
- **Have password recoveries sent to a secure email address.** You don't want hackers to know where your password reset messages are sent. Have these messages sent to an account you never use to send email.

Other techniques for obtaining login names and passwords are decidedly low-tech. Eavesdropping, such as simply looking over the shoulder of a legitimate computer user to learn their login name and password, is a common way that hackers gain access to computers. **Dumpster diving** means looking through garbage for interesting bits of information. Companies typically do not put a fence around their dumpsters. In midnight rummaging sessions, hackers have found user manuals, phone numbers, login names, and passwords. **Social engineering** refers to the manipulation of a

person inside the organization to gain access to confidential information. Social engineering is easier in large organizations where people do not know each other very well. For example, a hacker may identify a system administrator and call that person, pretending to be the supervisor of their supervisor and demanding to know why they can't access a particular machine. In this situation, a cowed system administrator, eager to please their boss's boss, may be talked into revealing or resetting a password [**6**].

Login credentials have been stolen from many organizations, and they are sold to hackers who try them on other sites. Every day, more than 20 million accounts are probed with stolen credentials. Hackers also gain login credentials through phishing attacks that trick users into revealing their passwords [7].

You probably have many online accounts. Choosing appropriate passwords for your accounts is a good first step (see sidebar). However, as the previous discussion makes clear, simply choosing a difficult-to-guess password is no longer sufficient to make your accounts reasonably secure. There are too many ways that hackers can gain access to this information.

To guard against hackers who have obtained your login credentials, you should set up your accounts to require multiple authenticators. **Multifactor authentication** is a protocol that requires two or more authenticators to verify a person's identity before giving them access to the requested service. For example, after verifying your login name and password, a multifactor authentication system will text you a six-digit code that you must enter before you can access your account. In this way, a hacker who obtains your login name and password but doesn't have access to your cell phone cannot access your account. According to Microsoft, enabling multifactor authentication blocks over 99.9 percent of account-compromising attacks [8].

7.2.2 Penalties for Hacking

Under US law, the maximum penalties for hacking are severe. The Computer Fraud and Abuse Act criminalizes a wide variety of hacker-related activities, including

- Transmitting code (such as a virus or worm) that causes damage to a computer system
- Accessing without authorization any computer connected to the Internet, *even if no files are examined,*

changed, or copied

- Transmitting classified government information
- Trafficking in computer passwords
- Computer fraud
- Computer extortion

The maximum penalty imposed for violating the Computer Fraud and Abuse Act is 20 years in prison and a $250,000 fine.

Another federal statute related to computer hacking is the Electronic Communications Privacy Act. This law makes it illegal to intercept telephone conversations, email, or any other data transmissions. It also makes it a crime to access stored email messages without authorization.

The use of the Internet to commit fraud or transmit funds can be prosecuted under the Wire Fraud Act and/or the National Stolen Property Act. Adopting the identity of another person to carry out an illegal activity is a violation of the Identity Theft and Assumption Deterrence Act.

7.2.3 Selected Hacking Incidents

Despite potentially severe penalties for convicted hackers, computer systems continue to be compromised by outsiders. Many break-ins are orchestrated by organized groups with a high degree of expertise, but others are committed by solo hackers who exploit a security weakness.

In 2003 a hacker broke into computers at the University of Kansas and copied the personal files of 1,450 international students studying in the United States. The files contained names, Social Security numbers, passport numbers, countries of origin, and birth dates. The University of Kansas had collected the information in one place in order to comply with a Patriot Act requirement that it report the information to the Immigration and Naturalization Service [9]. In a similar incident two years later, an intruder broke into a University of Nevada, Las Vegas, computer containing personal information on 5,000 international students studying in the United States [10].

In March 2005, someone discovered a security flaw in the online-admissions software produced by ApplyYourself and

used by six business schools. The discoverer posted instructions on a *Business Week* online forum explaining how business school applicants could circumvent the software security system and take a look at the status of their applications. It took ApplyYourself only nine hours to fix the flaw, but in the interim period hundreds of eager applicants had exploited the bug and peeked at their files. A week later, Carnegie Mellon University, Harvard University, and the Massachusetts Institute of Technology announced that they would not admit any of the applicants who had accessed their computer systems without authorization [**11**].

A hacker gained access to the *Sesame Street* channel on YouTube in October 2011, changed the home page, and replaced the videos with pornographic material. The site streamed the X-rated content for 22 minutes before Google could shut down the site [**12**].

7.2.4 FBI and the Locked iPhone

On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik brought assault rifles and semiautomatic handguns into the Inland Regional Center in San Bernardino, California, and opened fire at a holiday gathering, killing 14

people and seriously wounding 22 more. Around the time of the shooting Malik pledged allegiance to the Islamic State. Farook and Malik fled the event but died in a shootout with the police four hours later [**13**].

Farook and Malik, who were married, had destroyed their personal cell phones before leaving home, but the FBI recovered Farook's work-issued iPhone 5C. The FBI was eager to collect evidence from Farook's iPhone. The FBI obtained a warrant to search the contents of the phone, and the owner of the phone, Farook's employer, consented to the search. However, the iPhone was locked, and the FBI did not know the four-digit passcode. The iPhone's software was designed so that if ten consecutive incorrect passcodes were entered, the iPhone's encryption key would be erased, rendering all personal data stored on the iPhone permanently inaccessible. In February 2016 the FBI asked Apple to create a new version of the iOS operating system that would disable the ten-erroneous-passcode limit on the iPhone, as well as the feature that slows down subsequent passcode-entry attempts when incorrect passcodes are entered. When Apple refused to cooperate, the FBI convinced a US magistrate to issue an order for Apple to comply with the government's request [**14**]. Tim Cook, the CEO of Apple, responded to the court order by issuing a public statement that if Apple produced a

“backdoor” version of iOS that circumvented key security features, and that version fell into the wrong hands, it would enable criminals to unlock any iPhone they possessed [**15**]. The Department of Justice countered that the argument was fallacious because Apple could “maintain custody of the software” and “destroy it after its purpose under the Order has been served” [**14**]. Apple chose to fight the Department of Justice in court rather than comply with the FBI’s request. About a month later, before the case could go to trial, the Department of Justice stopped its legal effort to get Apple to cooperate, declaring that it had successfully unlocked Farook’s iPhone [**16**].

Two years later, a report by the inspector general of the Department of Justice revealed that the leader of the FBI’s Cryptographic and Electronic Analysis Unit, which was in charge of the investigation, decided to take legal action against Apple before thoroughly exploring whether another unit inside the FBI, the Remote Operations Unit, had the capability to unlock the phone without Apple’s help. Senator Ron Wyden of Oregon accused the FBI of being more interested in establishing a legal precedent than gaining access to the terrorist’s iPhone [**17**].

)

7.2.5 Case Study: Firesheep

Only a small fraction of the information transported by the Internet is encrypted; everything else is sent “in the clear” using the Hypertext Transfer Protocol (HTTP). Encrypting everything would make Internet communications slower and more expensive, which is why most Web sites use encryption only when communicating the most sensitive information, such as usernames, passwords, and credit card numbers. You can tell when a Web site is encrypting the communication because the start of the address in the Web browser is “https://” (meaning “secure Hypertext Transfer Protocol”).

The widespread use of Wi-Fi to connect to the Internet has exposed a vulnerability caused by Internet packets being sent in the clear. A Wi-Fi network uses radio signals to communicate between devices. If the wireless access point is not using encryption, it’s easy for devices within range to snoop on the network traffic. (Encryption is the process of protecting information by transforming it into a form that cannot be understood by anyone who does not possess the key, that is, the means of reversing the process and recreating the original information.)

Sidejacking is the hijacking of an open Web session by the capturing of a user's cookie, giving the attacker the same privileges as the user on that Web site. (You can find an explanation of cookies in Section 5.3.15.) Ecommerce Web sites typically use encryption to protect the username and password people provide when logging in, but they do not encrypt the cookie that the Web browser sends to the user to continue the session. Sidejacking is possible on unencrypted wireless networks because another device on the wireless network can "hear" the cookie being transmitted from the Web site back to the user's computer. Even though the Internet security community had known and complained about the sidejacking vulnerability for years, ecommerce Web sites did not change their practices.

On October 24, 2010, Eric Butler released an extension to the Firefox browser called Firesheep. Firesheep makes it easy for a Firefox user to sidejack open Web sessions. The user starts the Firefox browser, connects to an open Wi-Fi network, and clicks on a button called "Start Capturing." When someone using the network visits an insecure Web site that Firesheep knows about, the user's name and photo are displayed in a sidebar, along with the name of the Web site he is connected to, such as Amazon, Facebook, or Twitter. By double-clicking on the photo, the attacker becomes logged in

as that user on that Web site and is able to do the same things that the legitimate user is able to do, such as post status messages and purchase products.

Butler released Firesheep as free, open-source software for Mac OS X and Windows. In Butler's view, the organizations managing Web sites have a responsibility to protect the privacy of the people using those sites. Since the organizations had been ignoring this responsibility, it was time for users to step up and demand greater security. Firesheep was a way to help make that happen [**18**].

The Firesheep extension was downloaded more than 500,000 times in its first week of availability, and it attracted a great deal of media attention [**19**]. The typical story warned social network users about the dangers of using unencrypted wireless public networks and criticized the social network companies for not providing more security [**20**, **21**, **22**, **23**].

Responding to criticism for providing a tool that makes it easy for ordinary computer users to perform sidejacking, Butler pointed out that sidejacking tools had been available for years before he released Firesheep. He wrote, "Criminals already know this, and I reject the notion that something like Firesheep turns otherwise innocent people evil" [**24**].

Three months after Butler released Firesheep, Facebook made the following announcement:

> **Starting today we'll provide you with the ability to experience Facebook entirely over HTTPS. You should consider enabling this option if you frequently use Facebook from public Internet access points found at coffee shops, airports, libraries or schools. The option will exist as part of our advanced security features, which you can find in the "Account Security" section of the Account Settings page. [25]**

In March 2011, Twitter announced it was offering an "Always use HTTPS" option [**26**].

Act-Utilitarian Analysis

The release of Firesheep led the media to focus on the risks associated with the use of certain Web sites from unsecured wireless networks, and a few months later Facebook and Twitter made their Web sites more secure. There continues to be strong pressure for other Web services to follow suit. These are tremendous benefits for everyone who accesses the Web at a public Internet access point without encryption.

Butler was right when he predicted that Firesheep would not turn people into criminals. Even though half a million people downloaded Firesheep in the first week, there was no evidence of a big increase in identity theft or even malicious pranks. The harms caused by Firesheep appeared to be minimal. Because the release of Firesheep caused great benefits and negligible harm, we conclude it was a good action from a utilitarian point of view.

Virtue-Ethics Analysis

Butler demonstrated civic responsibility by using his technical skills to develop Firesheep, a piece of software that dramatically illustrated, even to nontechnical people, the lack of security when unencrypted HTTP messages are sent over an unencrypted Wi-Fi network. On the day he released Firesheep, Butler pointed out on his blog that side-jacking attacks are simple to execute because cookies are wirelessly broadcast without encryption. Web sites haven't eliminated this problem even though it has been discussed for a long time. He continued:

> **Facebook is constantly rolling out new "privacy" features in an endless attempt to quell the screams of unhappy users, but what's**

> **the point when someone can just take over an account entirely?** [18]

Butler explained that he released Firesheep to point out the gravity of the problem [18]. Responding to criticisms of his action, he stated emphatically that it is wrong for anyone to harm another person. He did not create Firesheep to facilitate evil; instead, his goal was to make people aware of a problem that had been ignored for too long [24]. All of these statements are characteristic of someone truly interested in protecting the privacy of visitors to popular Web sites. Butler exhibited courage by taking personal responsibility for creating Firesheep, and he demonstrated benevolence by making it freely available.

Therefore, from the perspective of virtue ethics, Butler's actions and statements were characteristic of someone interested in promoting the common good. He seemed to sincerely believe that something significant needed to be done to get the companies to change their privacy policies.

Kantian Analysis

To begin with, accessing someone else's user account is an invasion of that person's privacy and is wrong. Butler clearly

agrees with this perspective because he refers to people who sidejack accounts as “evil.” Butler’s goal was to pressure Facebook, Twitter, Amazon, and other Web sites to adopt proper security measures to protect their users. He saw the best way to achieve this end was to release a tool that would bring to light a well-known security problem that had not gotten sufficient attention.

Criminals already knew how to sidejack Web sessions before Butler created Firesheep. What Firesheep did was make sidejacking so simple that even ordinary computer users could do it. More than half a million copies of Firesheep were downloaded in the first week, and undoubtedly some of these people actually used the software to sidejack Web sessions, which is wrong. It is disingenuous for Butler to “reject the notion that something like Firesheep turns otherwise innocent people evil.” He provided a tool that made it much simpler for people to do something that is wrong, and therefore he has some moral accountability for the misdeeds of the people who downloaded Firesheep.

Ultimately, Butler was willing to tolerate a short-term increase in privacy violations in the hope that users would pressure Facebook, Twitter, and other sites to improve their security, which would result in fewer privacy violations in the

long term. In other words, he was willing to use the people targeted by Firesheep as a means to his end. From a Kantian perspective, it was wrong for Butler to release Firesheep to the public.

There are other ways Butler could have achieved his goal without using other people. For example, he could have gone on a popular television show and hacked into the host's Facebook page, generating a great amount of publicity without having to release the software [27].

7.3 Malware

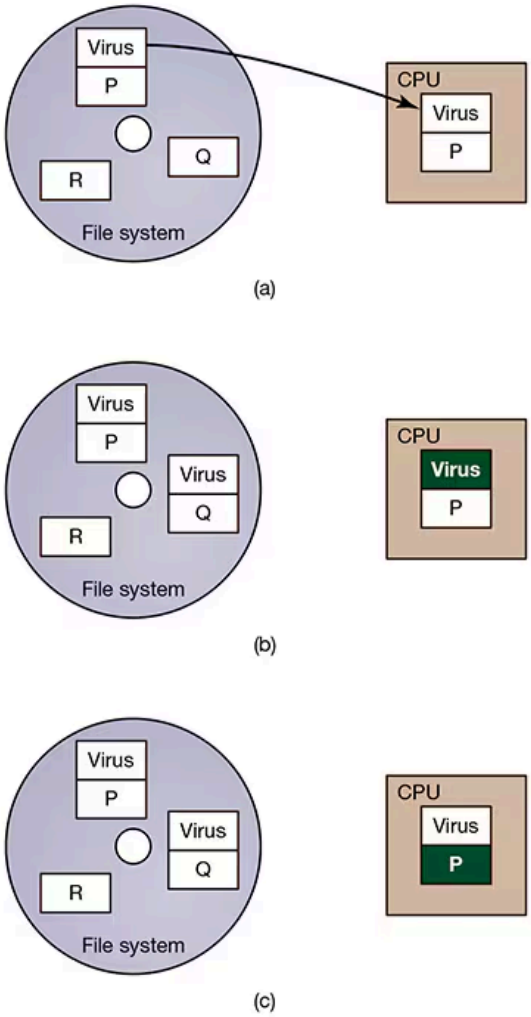
The Firesheep extension to the Firefox browser highlights a significant security weakness of unencrypted Wi-Fi networks. Computers have security weaknesses, too, and there are a variety of ways in which malicious software, or **malware**, can become active on your computer. If you are lucky, these programs will do nothing other than consume a little CPU time and some disk space. If you are not so lucky, they may destroy valuable data stored in your computer's file system. An invading program may even allow outsiders to seize control of your computer. Once this happens, they may use your computer as a depository for stolen credit card information, a Web server dishing out pornographic images, or a launch pad for spam or a denial-of-service attack on a corporate or government server.

7.3.1 Viruses

Viruses represent one way in which malicious code can get into a computer. A **virus** is a piece of self-replicating code embedded within another program called the **host** [28]. Figure 7.1 illustrates how a virus replicates within a computer. When a user executes a host program infected

with a virus, the virus code executes first. The virus finds another executable program stored in the computer's file system and replaces the program with a virus-infected program. After doing this, the virus allows the host program to execute, which is what the user expected to happen. If the virus does its work quickly enough, the user may be unaware of the presence of the virus.

Figure 7.1



One way a computer virus can replicate. (a) A computer user executes program P, which is infected with a virus. (b) The virus code begins to execute. It finds another executable program Q and creates a new version

of Q infected with the virus. (c) The virus passes control to program P. The

Because a virus is attached to a host program, you may find viruses anywhere you can find program files: hard disks, thumb drives, CD-ROMs, email attachments, and so on. Viruses can be spread from machine to machine via thumb drives or CDs. They may also be passed when a person downloads a file from the Internet. Sometimes viruses are attached to free computer games that people download and install on their computers.

Today many viruses are spread via email attachments (Figure 7.2). We are all familiar with ordinary attachments such as photos, but attachments may also be executable programs or word-processing documents or spreadsheets containing macros, which are small pieces of executable code. If the user opens an attachment containing a virus, the virus takes control of the computer, reads the user's email address book, and uses these addresses to send virus-contaminated emails to others, as illustrated in Figure 7.3.

Figure 7.2

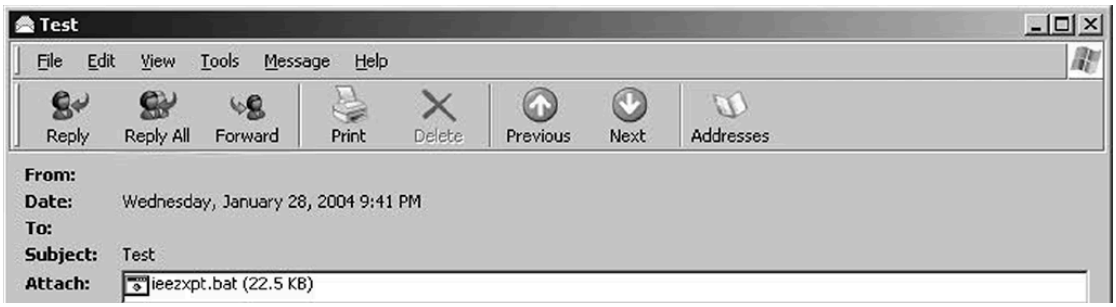
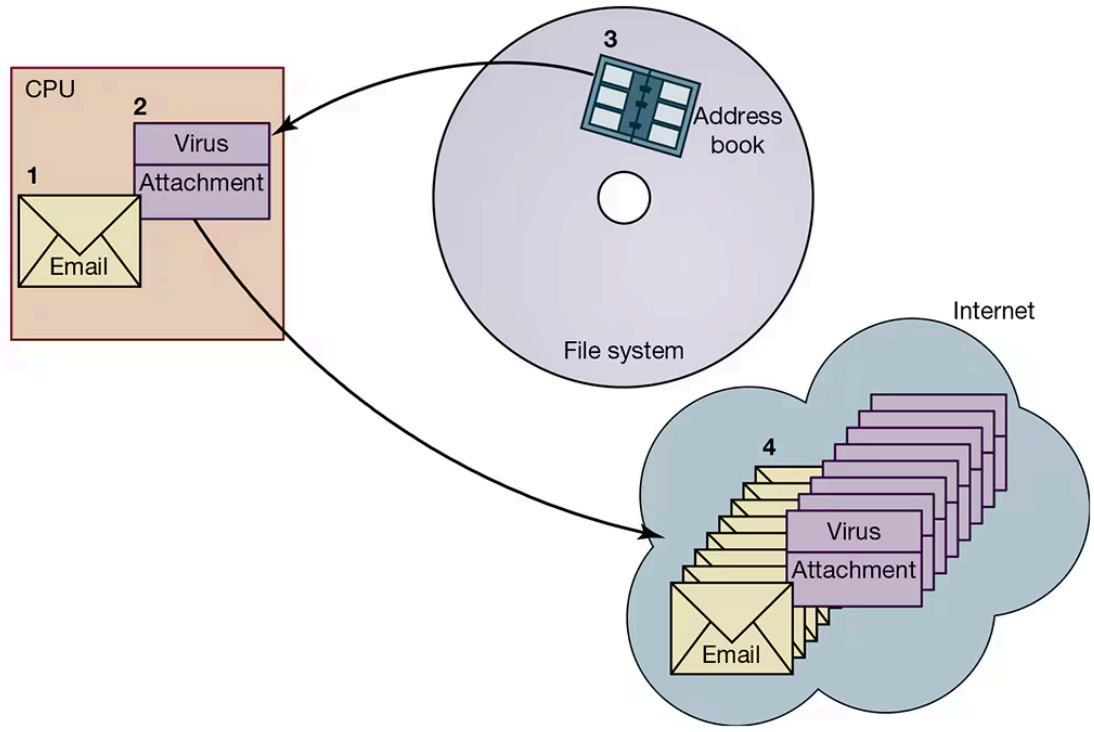


Figure 7.3



How an email virus spreads. A computer user reads an email with an attachment (1). The user opens the attachment, which contains a virus (2). The virus reads the user's email address book (3). The virus sends emails with virus-containing attachments (4).

Some viruses are fairly innocent; they simply replicate. These viruses occupy disk space and consume CPU time, but the harm they do is relatively minor. Other viruses are malicious and can cause significant damage to a person's file system.

Commercial antivirus software packages allow computer users to detect and destroy viruses lurking on their

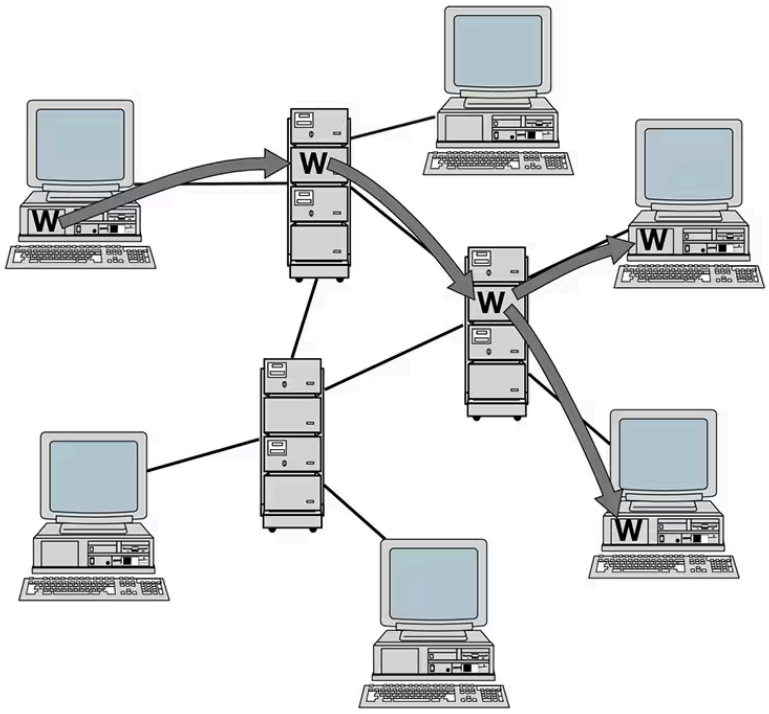
computers. To be most effective, users must keep antivirus software up-to-date by downloading patterns corresponding to the latest viruses from the vendor's Web site. Unfortunately, many people are negligent about keeping their virus protection software up-to-date. According to the statistics office of the European Union, a survey of Internet users revealed that 31 percent of them had experienced a computer virus in the previous 12 months that had resulted in a loss of information or time, even though 84 percent of them said that their computer was running antivirus software [**29**]. That means they were not keeping their virus protection current.

To make matters worse, criminals have found a way to profit from people's concern about viruses and their eagerness to install antivirus software when they believe their systems are infected. In July 2011, more than two million PCs were infected with a fake antivirus application that actually routed traffic destined for Google through intermediate servers controlled by the attacker. The purpose of the malware appeared to be to generate "click-through" income for the hackers by directing people to Web sites containing fake security programs [**30**].

7.3.2 The Internet Worm

A **worm** is a self-contained program that spreads through a computer network by exploiting security holes in the computers connected to the network (Figure 7.4). The technical term "worm" comes from *The Shockwave Rider*, a 1975 science-fiction novel written by John Brunner [**31**].

Figure 7.4



A worm spreads to other computers by exploiting security holes in computer networks.

The most famous worm of all time was also the first one to get the attention of the mainstream media, which is why it is popularly known as the Internet worm, even though many other worms have been created that propagate through the

Internet. The primary source for this narrative is the excellent biography of Robert Morris in *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, written by Katie Hafner and John Markoff [**32**].

Background of Robert Tappan Morris Jr.

Robert Tappan Morris Jr. began learning about the Unix operating system when he was still in junior high school. His father was a computer security researcher at Bell Labs, and young Morris was given an account on a Bell Labs computer that he could access from a teletype at home. It didn't take him long to discover security holes in Unix. In a 1982 interview with Gina Kolata, a writer for *Smithsonian* magazine, Morris admitted he had broken into networked computers and read other people's email. "I never told myself that there was nothing wrong with what I was doing," he said, but he acknowledged that he found breaking into systems challenging and exciting, and he admitted that he continued to do it.

As an undergraduate at Harvard, Morris majored in computer science. He quickly gained a reputation for being the computer lab's Unix expert. After his freshman year,

Morris worked at Bell Labs. The result of his work was a technical paper describing a security hole in Berkeley Unix.

While at Harvard, Morris was responsible for several computer pranks. In one of them, he installed a program that required people logging in to answer a question posed by "the Oracle" and then to ask the Oracle another question. (The Oracle program worked by passing questions and answers among people trying to log in.)

Designing the Worm

Morris entered the graduate program in computer science at Cornell University in the fall of 1988. He became intrigued with the idea of creating a computer worm that would exploit bugs he had found in three Unix applications: `ftp`, `sendmail`, and `fingerd`. His "wish list" for the worm had about two dozen goals, including the following:

- Infect three machines per local area network
- Only consume CPU cycles if the machines are idle
- Avoid slow machines
- Break passwords in order to spread to other computers

The goal of the worm was to infect as many computers as possible. It would not destroy or corrupt data files on the machines it infected.

Launching the Worm

On November 2, 1988, Morris learned that a fix for the `ftp` bug had been posted to the Internet, meaning his worm program could no longer take advantage of that security hole. However, nobody had posted fixes to the other two bugs Morris knew about. After making some last-minute changes to the worm program, he logged into a computer at the MIT Artificial Intelligence Lab and launched the worm from that computer at about 7:30 p.m.

The worm quickly spread to thousands of computers at military installations, medical research facilities, and universities. Unfortunately, due to several bugs in the worm's programming, computers became infected with hundreds of copies of the worm, causing them to crash every few minutes or become practically unresponsive to the programs of legitimate users.

Morris contacted friends at Harvard to discuss what ought to be done next. They agreed that Andy Sudduth would anonymously post a message to the Internet. Sudduth's

message is shown here.[1] Harvard's computers were not affected (the security holes had already been patched), and you can tell from the last sentence that Sudduth was having a hard time believing Morris's story:

> A Possible virus report:
>
> There may be a virus loose on the internet. Here is the gist of a message I got:
>
> I'm sorry.
>
> Here are some steps to prevent further transmission:
>
> 1) don't run finger, or fix it to not overrun its stack when reading arguments. 2) recompile sendmail w/o DEBUG defined 3) don't run rexed
>
> Hope this helps, but more, I hope it is a hoax.

Sudduth's email was supposed to get routed through a computer at Brown University. However, computers at Brown were already infected with the worm and did not have spare cycles to route the message. Also, the email did not have a subject line, which made it less likely to be read during a crisis. The result is that the message was read too late to be of any help to those fighting the worm.

System administrators at various universities worked frantically to stop the spread of the worm. Within a day they had examined the worm's code, discovered the bugs in `sendmail` and `fingerd`, and published fixes to the Internet community. No one knows exactly how many computers were infected by the worm, but it did make a significant number of systems unusable for a day or two [33].

After some sleuthing by reporter John Markoff, the *New York Times* named Robert Tappan Morris Jr. as the author of the worm. Morris was suspended from Cornell University. A year later, he was the first person to receive a felony conviction under the US Computer Fraud and Abuse Act. He was sentenced to three years' probation and 400 hours of community service, and was fined $10,000. His legal fees and fines exceeded $150,000.

Ethical Evaluation

Was Robert Morris Jr. wrong to unleash the Internet worm?

A Kantian evaluation must focus on Morris's will. Did Morris have good will? His stated goal was to see how many Internet computers he could infect with the worm. While Morris did not want to crash these computers or destroy any data stored on them, his motivation was fundamentally

selfish: he wanted the thrill of seeing his creation running on thousands of computers. He used others because he gained access to their machines without their permission. There is also evidence Morris knew he was using others: he took measures designed to prevent people from discovering that he was the author of the worm. From a Kantian point of view, Morris's action was wrong.

From a social-contract point of view, Morris's action was also wrong. He violated the property rights of the individuals and organizations whose computers were infected by the worm. They had the right to determine who would use their computers, and they attempted to enforce this right by requiring people to identify themselves by user-name and password. Morris took advantage of security holes in these computers to gain unauthorized access to them. When his worm caused these computers to become unresponsive or crash, he denied access to the legitimate users of these computers.

A utilitarian evaluation of the case focuses on the benefits and harms resulting from the spread of the worm. The principal benefit of the Internet worm was that organizations managing these Unix computers discovered there were two significant security holes in their systems. They received the

instructions they needed to patch these holes before a truly malicious intruder took advantage of them to enter their systems and do a lot of damage to their data. Of course, Morris could have produced the same beneficial result simply by contacting the system administrators at UC Berkeley and informing them of the security holes he had found.

The Internet worm had numerous harmful consequences. A large amount of time was spent by system administrators as they defended their machines from further attacks, tracked down the problem, installed patches, and brought machines back on line. There was a disruption in email and file-exchange traffic caused by computers being taken off the network. About 6,000 computers were unavailable for a day or two. During this time, many thousands of people were less productive than they could have been had the systems been up and running. Morris himself was harmed by his actions. He was suspended from Cornell and convicted of a felony, which resulted in a sentence of probation, community service, and a substantial fine.

Considering all of Morris's options, it is clear that another course of action—simply alerting the Unix community to the bugs—would have produced all of the benefits with none of

the harms. Therefore, from a utilitarian viewpoint, Morris was wrong to have released the Internet worm.

From the perspective of virtue ethics, Morris's actions are not consistent with those of a virtuous person. He selfishly chose to use the Internet as an experimental laboratory, and he deceitfully released the worm from MIT rather than Cornell University. When the worm began spreading uncontrollably, he avoided taking responsibility for his actions by asking a trusted friend to post the message to the Internet explaining how to fight the worm.

In conclusion, Morris may not have been acting maliciously, but he was acting selfishly. If he had wanted to experiment with worms, he probably could have gotten permission to try out his creations on a local area network detached from the Internet, so that even if his worm multiplied out of control, there would have been no fallout to the rest of the computer community. Instead, he chose to use the entire Internet as his experimental laboratory, inconveniencing thousands of people.

7.3.3 Cross-Site Scripting

Cross-site scripting is another way in which malware may be downloaded without a user's knowledge. Web sites that

allow users to read what other users have posted are vulnerable to this security problem. The attacker injects a client-side script into a Web site. When an innocent user visits the site sometime later, the user's browser executes the script, which may steal cookies, track the user's activity, or perform another malicious action.

7.3.4 Drive-By Downloads

Many malware creators have hacked into legitimate Web sites and installed software booby traps. In some cases, simply visiting a compromised Web site can result in the unintentional downloading of software, called a **drive-by download**. Another kind of drive-by download occurs when a Web surfer encounters a pop-up window asking permission to download software. The user approves the download, thinking the code is necessary to view the content on the Web site, but in actuality the download contains malware.

7.3.5 Trojan Horses and Backdoor Trojans

A **Trojan horse** is a malicious computer program designed to deceive users by concealing a sinister purpose behind a

benign capability. When the user executes a Trojan horse, the program performs the expected beneficial task. However, the program is also performing actions unknown to, and not in the best interests of, the user.

An example of a Trojan horse is Mocmex, first uncovered in 2008 in digital picture frames manufactured in China. It spread from digital picture frames to computer hard drives and other portable storage devices people attached to their PCs. The purpose of the Trojan horse appeared to be to steal passwords to online computer games [**34**].

A **backdoor Trojan** is a Trojan horse that gives the attacker access to the another person's computer. For example, a backdoor Trojan may purport to cleanse malware from a computer, but in actuality it installs spyware (described later).

7.3.6 Ransomware

Ransomware is malware designed to extort money from the person targeted by the attack. It may be installed on a targeted person's computer via a drive-by download, a Trojan horse, an email attachment, or another means. The

ransomware problem began in Russia but began spreading in a significant way to other countries in 2012 [35].

Early versions of ransomware often used a phony message from a law enforcement agency to accuse targeted persons of an illegal activity and to extract "fines" from them. For example, Reveton locked the targeted person's computer and filled the screen with a window containing a message purporting to be from the FBI or the Department of Justice. The message informed targeted persons that their IP address had been associated with some sort of illegal activity, such as downloading child pornography, and demanded that they pay a fine using a prepaid money card [36].

Today, cryptographic ransomware is a serious problem, particularly for businesses. Cryptographic ransomware encrypts all of the files on the targeted person's computer and demands payment in return for the key that can be used to decrypt the files. In 2015 the FBI reported that it had been contacted by 992 persons targeted by CryptoWall ransomware, who had paid over $18 million (or about $18,000 per business) to ransom their files. The FBI estimated the total number of businesses attacked by CryptoWall to be much larger because not every targeted

person filed a report with the FBI, and some businesses abandoned their files rather than pay the ransom [37].

7.3.7 Rootkits

A **rootkit** is a set of programs that provide privileged access to a computer. Once installed, a rootkit is activated every time the computer is booted. Rootkits are difficult to detect because they start running before the operating system has completed booting up, and they can use security privileges to mask their presence.

7.3.8 Spyware and Adware

Spyware is a program that communicates over an Internet connection without the user's knowledge or consent. Spyware programs can monitor Web surfing, log keystrokes, take snapshots of the computer screen, and send reports back to a host computer. Spyware is often part of a rootkit. **Adware** is a type of spyware that displays pop-up advertisements related to what the user is doing.

Since people would not intentionally download a spyware program, spyware must get installed using subterfuge. Free software downloaded from the Internet often contains

spyware. Alternatively, the spyware may be a Trojan horse, tricking users into downloading it because they think it serves a useful purpose. A Trojan horse containing spyware is an example of a backdoor Trojan. A 2006 survey of US consumers with broadband Internet connections found that 89 percent of them had spyware on their computers [38].

7.3.9 Bots and Botnets

A **bot** is a particular kind of backdoor Trojan that responds to commands sent by a command-and-control program located on an external computer. The first bots supported legitimate applications: Internet Relay Chat channels and multiplayer Internet games. Today, however, bots are frequently used to support illegal activities. A collection of bot-infected computers is called a **botnet**, and a person who controls a botnet is called a **bot herder**. Botnets can range in size from a few thousand computers to over a million computers. In most cases, people have no idea that their PCs have been compromised and are part of a botnet.

It's been estimated that as much as 90 percent of spam is distributed through botnets [39]. Bots can also be used as spyware, stealing files or logging keystrokes to gain credit card numbers or other sensitive information. Botnets can also

be used to support distributed denial-of-service attacks, which we discuss in Section 7.4.3.

The sophistication of bots continues to increase. Computers typically have signature-based detection schemes to identify and destroy bots by looking for particular patterns in their underlying machine code. To counter these detection schemes, programmers are now creating bots that are able to spin off functionally equivalent bots with somewhat different machine code.

Sidebar: Protect Your Internet-Connected Devices

You can greatly reduce the chances that malware will infect your computer or your other Internet-connected devices. Taking these steps will help protect your personal information and help keep your devices from being co-opted into botnets.

- **Make sure your computers have the latest security patches installed.** Most malware exploits vulnerabilities for which security

patches have already been created. That means they can only infect those computers that have not been kept up-to-date with the latest patches.

- **Install anti-malware tools on your personal computer.** Anti-malware tools are designed to protect computers against malware, such as viruses, worms, Trojan horses, adware, and spyware. Anti-malware software can be used to scan a computer's hard drive, detecting files that appear to contain viruses or spyware, and deleting the files (with the user's approval).

- **Before you purchase a device that connects to the Internet, make sure its manufacturer is taking reasonable security precautions.** There are now an amazing number of devices you can connect to the Internet. Printers, thermostats, doorbells, security cameras, baby monitors, pet feeders, fire alarms, and garage door openers are just a few examples of the technology called the Internet of Things (IoT). Any IoT device you purchase should allow you to change its password. The best devices

make it easy to download security updates [40].

- **When you purchase an IoT device, immediately change the password.** An IoT device without a secure password can become compromised by malware within minutes of being connected to the Internet. Change the device's password before you use the device, and choose a secure password (see the previous sidebar) [40].

  If you are changing the default password of an IoT device you have been using for a while, turn the device off for 30 seconds after you have changed the password. Disconnecting the power will erase the device's memory, often removing any malware that may have infected it [40].

- **Choose a different password for each of your devices.** By doing so, even if a malevolent agent should guess the password of one of your devices, the rest of your devices will still be secure [40].

- **Consider replacing insecure IoT devices.** If you cannot change the administrator password of your device or update its firmware, you should consider disconnecting the device from the Internet and purchasing a newer device with greater security [40].

7.3.10 Security Risks Associated with "Bring Your Own Device"

Increasingly, companies are allowing employees to bring personal smartphones, tablets, and laptops to the workplace and use them for work-related activities. In fact, a survey of US companies with more than 100 employees revealed that 87 percent of them depend on employees accessing mobile business apps from their personal smartphones [41].

The "bring your own device" (BYOD) movement brings numerous benefits. Employers can reduce their hardware and software expenditures. Employees can use devices they are

more comfortable with, increasing their productivity and job satisfaction. However, allowing employees to use their own devices to access the company network, send and receive email, or access company data introduces security risks.

One of these risks is that company data may be compromised if the employee's device is stolen. Some companies have begun encrypting all data files, to prevent a data breach even if a personal device containing company data is stolen [**42**].

Another risk is that if the employee's device is insecure, it may provide an avenue for a malevolent agent to break into the company's network. For example, in 2017 hackers broke into the personal computer of an employee of Bithumb, a South Korean digital currency exchange, and used the PC to access company files and steal personal data of about 30,000 Bithumb customers [**43**].

To address security concerns, companies establish BYOD policies [**42**]. These policies can address a variety of issues, including:

- What are the security standards for personal devices (password requirements, anti-malware packages, etc.)?
- What applications are employees allowed to run from their personal devices?

- What is the level of support for personal devices that the company's IT department will provide?
- Does the company have the right to erase all data on a personal device that has been stolen?
- How will company data be removed from the devices of employees who are leaving the company?

Possible Virus Report by Ruth Kennedy Sudduth. Copyright © by Ruth Kennedy Sudduth. Used by permission of Ruth Kennedy Sudduth.

7.4 Cyber Crime and Cyber Attacks

The Internet plays a vital role in the economic life of developed nations. Its effects include streamlining interactions between manufacturers and their suppliers, stimulating the creation of new companies, fostering the development of new business models, making online videoconferencing much more affordable, and changing how people shop. Today, there are more than 80 million dot-com domains. Annual ecommerce sales now exceed $5 trillion [**44**]. Given the amount of money changing hands, it's not surprising that organized crime is active on the Internet. The economic importance of Internet-based activities also makes Internet infrastructure an attractive target for politically motivated attacks.

We begin this section by reviewing three common Internet-based attacks. We then explore how these attacks have been used as a means to achieve criminal or political ends.

7.4.1 Phishing and Spear Phishing

A **phishing** (pronounced "fishing") attack is a large-scale effort to gain sensitive information from gullible computer users. An attacker sends out millions of email messages from a botnet. The messages inform the recipients that one of their accounts has been compromised and directs them to connect to a Web site to resolve the problem. Targeted users that click on the link encounter an impostor Web site designed to resemble the genuine ecommerce site. Once on the site, they are asked for a login name, password, and other private information. Information collected by the impostor site can then be used for identity theft.

According to an industry study, there were at least 123,972 phishing attacks worldwide in the second half of 2014. An interesting development is the increase in phishing attacks on Chinese ecommerce sites, indicating the growing importance of the Chinese economy [**45**].

Spear phishing is a variant of phishing in which the attacker selects email addresses that target a particular group of recipients or even one particular person. For example, an

attacker may target older people they have assumed to be more gullible or members of a group that have access to valuable information [**46**].

John Podesta, the chairman of Hillary Clinton's presidential campaign, is a famous recipient of a spear-phishing attack. On March 19, 2016, Podesta received an email, apparently from Google, that addressed him by name and contained the ominous message, "Someone just used your password to try to sign in to your Google Account." The message went on to say, "Google stopped this sign-in attempt. You should change your password immediately." When Podesta clicked on the "CHANGE PASSWORD" box and provided his old and new passwords, he gave Russian hackers access to his account. In October of 2016, thousands of Podesta's emails were published on WikiLeaks. Former secretary of state Colin Powell suffered a similar attack, and he, too, had some of his private emails published on the Web during the 2016 presidential campaign [**47**, **48**].

7.4.2 SQL Injection

SQL injection is a method of attacking a database-driven Web application that has improper security. The attacker accesses the application like any other client of the

application, but by inserting (injecting) an SQL query into a text string from the client to the application, the attacker can trick the application into returning sensitive information.

7.4.3 Denial-of-Service and Distributed Denial-of-Service Attacks

A **denial-of-service (DoS) attack** is an intentional action designed to prevent legitimate users from making use of a computer service [49]. A DoS attack may involve unauthorized access to one or more computer systems, but the goal of a DoS attack is not to steal information. Instead, the aim of a DoS attack is to disrupt a computer server's ability to respond to its clients. Interfering with the normal use of computer services can result in significant harm. A company selling products and services over the Internet may lose business. A military organization may find its communications disrupted. A government or nonprofit organization may be unable to get its message out to the public.

A DoS attack is an example of an "asymmetric" attack, in which a single person can harm a huge organization, such as

a multinational corporation or even a government. Since terrorist organizations specialize in asymmetric attacks, some fear that DoS attacks will become an important part of the terrorist arsenal [50, 51].

In a **distributed denial-of-service (DDoS) attack**, the attacker rents access to a botnet from a **bot herder**. At the selected time, the command-and-control computer sends the appropriate instructions to the bots, which launch their attack on the targeted system.

7.4.4 Internet-of-Things Devices Co-opted for DDoS Attack

On October 21, 2016, a DDoS attack against domain name service provider Dyn caused Netflix, Twitter, Spotify, Reddit, PayPal, Pinterest, and media organizations CNN, Fox News, the Guardian, the New York Times, and the Wall Street Journal to become unreachable for several hours [52]. Dyn provides the important service of translating domain names into numerical IP addresses. When Dyn was swamped with bogus requests from an enormous botnet, legitimate requests could not be serviced. What made the DDoS attack

noteworthy was that it was launched by the Mirai botnet, which consists of malware-infected Internet-of-Things (IoT) devices, such as network routers, security cameras, and baby monitors. The DDoS attack on Dyn was particularly powerful—executed by as many as 100,000 devices [53].

IoT devices are relatively easy for malicious actors to co-opt because many people install them without changing their passwords from the factory default settings. Some inexpensive devices come with no password protections at all. As a result, millions of IoT devices may already be infected by malware [54].

7.4.5 Cyber Crime

Criminal organizations have discovered that a great deal of money can be made from malware, so many of them have entered the arena, raising the stakes for corporations and individuals trying to protect their systems and sensitive information, respectively. Edward Skoudis paints a grim picture of the contemporary landscape:

> **Some attackers sell to the highest bidder customized malicious code to control victim machines. They may rent out armies of**

> infected systems useful for spam delivery, phishing schemes, denial-of-service attacks, or identity theft. Spyware companies and overly aggressive advertisers buy such code to infiltrate and control victim machines. A single infected machine displaying pop-up ads, customizing search engine results, and intercepting keystrokes for financial accounts could net an attacker $1 per month or more. A keystroke logger on an infected machine could help the attacker gather credit card numbers and make $1,000 or more from that victim before the fraud is discovered. With control of 10,000 machines, an attacker could set up a solid profit flow from cyber crime. Organized crime groups may assemble collectives of such attackers to create a business, giving rise to a malicious code industry. In the late 1990s, most malicious code publicly released was the work of determined hobbyists, but today, attackers have monetized their malicious code; their profit centers throw off funds that can be channeled into research and development to create more powerful malicious software and refined business models, as well as to fund other crimes. [46]

In the remainder of this section, we review a few well-known cyber crime incidents.

Jeanson James Ancheta

In 2004 and 2005, Internet café employee Jeanson James Ancheta created a network of about 400,000 bots, including computers operated by the US Department of Defense. Adware companies, spammers, and others paid Ancheta for

the use of these computers. After being arrested by the FBI, Ancheta pleaded guilty to a variety of charges, including conspiring to violate the Computer Fraud Abuse Act and the CAN-SPAM Act. In May 2006, a federal judge sentenced Ancheta to 57 months in prison and required him to pay $15,000 in restitution to the US government for infecting Department of Defense computers. Ancheta also forfeited to the government the proceeds of his illegal activity, including his 1993 BMW, more than $60,000 in cash, and his computer equipment [**55**, **56**].

Pharmamaster

Israeli company Blue Security created a spam-deterrence system for people tired of receiving unwanted email. Blue Security sold the service to businesses, but individuals could protect their home computers for free. About half a million people signed up for this free service. Users loaded a bot called Blue Frog on their computers. The bot integrated with Yahoo Mail, Gmail, and Hotmail, checking incoming email messages for spam. When it discovered a spam message, the bot would contact a Blue Security server to determine the source of the email. Then the bot would send the spammer an opt-out message [**57**].

Spammers who indiscriminately sent emails to millions of addresses started receiving hundreds of thousands of opt-out messages, disrupting their operations. Six of the world's top ten spammers agreed to use Blue Security's filtering software to remove Blue Frog users from their email lists [57].

One spammer, nicknamed PharmaMaster, did not back down. He threatened Blue Frog users with messages such as this one: "Unfortunately, due to the tactics used by Blue Security, you will end up receiving this message or other nonsensical spams 20–40 times more than you would normally" [39]. He followed through on his threats on May 1, 2006, by sending Blue Frog users 10–20 times as much spam as they would normally receive [57].

The next day PharmaMaster went after Blue Security itself. He launched a massive DDoS attack from tens of thousands of bots targeting Blue Security's servers. The huge torrent of incoming messages disabled the Blue Frog service. Later DDoS attacks focused on other companies providing Internet services to Blue Security. Finally, the spammer targeted the businesses that paid for Blue Security's services. When Blue Security realized it could not protect its business customers from DDoS attacks and virus-laced emails, it reluctantly discontinued its service. "We cannot take the responsibility

for an ever-escalating cyberwar through our continued operations," wrote Eran Reshef, CEO of Blue Security. "We are discontinuing all of our anti-spam activities" [57]. Blue Security's decision to fight bots with bots—always controversial—was ultimately unsuccessful.

Albert Gonzalez

In 2010 Albert Gonzalez was sentenced to 20 years of imprisonment after pleading guilty to using an SQL injection attack to steal more than 130 million credit and debit card numbers. Some of the credit and debit card numbers were sold online, leading to unauthorized purchases and bank withdrawals. The targets of the attacks were Heartland Payment Systems, 7-Eleven, Hannaford Brothers Supermarkets, TJX, DSW, Barnes & Noble, OfficeMax, and the Dave & Buster's chain of restaurants. Most of the numbers were stolen from Heartland Payment Systems, which estimated its losses at $130 million [58, 59].

Avalanche Gang

The Avalanche Gang is the name given to the criminal enterprise responsible for more phishing attacks than any other organization. The Anti-Phishing Working Group (APWG) estimated that the Avalanche Gang was responsible

for two-thirds of all global phishing attacks launched in the second half of 2009. In the second half of 2010, APWG noticed that Avalanche had nearly ceased its phishing attacks, leading APWG to speculate that Avalanche was changing strategies and focusing on the propagation of spam that tricks people into downloading the Zeus Trojan horse [**60**].

Colonial Pipeline

The Colonial Pipeline is one of the largest pipelines in the United States. Nearly half of all fuel used on the East Coast is transported from Texas through the Colonial Pipeline [**61**]. On May 6, 2021, hackers gained access to the Colonial Pipeline Company's administrative computing system by leveraging a reused password exposed in another data breach. The attackers downloaded nearly 100 gigabytes of data. The next day, the hackers conducted a ransomware attack. They encrypted the data on the company's hard drives and demanded a ransom of 75 Bitcoins, worth more than $4 million.

There is no evidence the hackers had access to the computers controlling the actual pipeline, but without the ability to bill its customers, the company immediately shut down the pipeline until it could restore its billing system [**62**].

The company, working with the FBI, paid the ransom to get a decryption tool from the attackers. The company immediately got to work restoring its computer systems. The decryption tool turned out to be so slow that the company found it quicker to restore its systems from backups [**63**].

As the shutdown continued, people began panic buying gasoline, prices jumped, and some gasoline stations ran out fuel [**64**]. Restarting the pipeline began on May 12 and took several days.

The FBI identified the hacker group DarkSide as responsible for the ransomware attack. A month after the ransomware attack, the Department of Justice announced that the FBI had recovered 63.7 Bitcoins of the ransom payment. The Department of Justice did not explain how the FBI had gained access to the private key needed to access the Bitcoins [**65**].

7.4.6 Politically Motivated Cyber Attacks

A **cyber attack** is a "computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it" [**66**]. Some nation-

states, terrorist organizations, and allied groups are mounting politically motivated cyber attacks on the computer and network infrastructure of their opponents, and some of these efforts have caused major disruptions.

Estonia (2007)

The small Baltic country of Estonia was part of the Soviet Union from the end of the Second World War until it became independent in 1991, and ethnic Russians still make up about a quarter of its population. In the capital city of Tallinn, a large bronze statue of a Soviet soldier had long been a point of controversy between Estonians and Russians. Russians saw it as a symbol of the sacrifices made by Soviet troops in the victory over Germany in the Great Patriotic War, while Estonians saw it as a symbol of the oppressive Soviet occupation.

After 16 years of independence, the Estonian government decided to relocate the controversial statue from downtown Tallinn to a Russian military cemetery in the suburbs. They knew the relocation would be hugely unpopular with the Russians. In fact, the Russian government had warned that removing the statue would be "disastrous for Estonians" [67]. The police were prepared for violence, and although

ethnic Russians rioted for two nights after the statue was moved, the damage was limited.

The government also expected an attack on its cyber infrastructure. Sure enough, an attack came, but its magnitude was greater than anything expected by the government's Internet security group. DDoS attacks from nearly a million computers targeted Estonian government ministries and all of Estonia's major commercial banks, telecommunications companies, and media outlets. To combat the attacks, much of Estonia's Internet was made inaccessible to computers outside the country, and on May 10, 2007, Estonia's largest bank had to suspend online services for an hour [**67**, **68**].

In 2009 a group of Russian activists connected with Nashi, a pro-Kremlin youth group, claimed responsibility for the cyber attacks [**69**].

Georgia (2008)

Georgia is another former Soviet republic that gained independence in 1991. South Ossetia, a region of Georgia adjacent to Russia, gained de facto autonomy from Georgia after a brief war in 1991, though it continues to be recognized as a part of Georgia by the international

community. On August 7, 2008, after provocations by South Ossetian separatists, Georgia sent troops into South Ossetia. Russian forces entered South Ossetia on August 8, and Russian and Georgian troops fought in South Ossetia for four days. A cease-fire between Georgia and Russia was signed a week later.

The conflict between Georgia and Russia is notable because even before Russian troops had entered South Ossetia, the Georgian government suffered a series of DDoS attacks that affected its ability to communicate with the outside world. Multiple Web sites went down for hours. The Georgian government went so far as to switch some of its Web hosting locations to the United States. American security experts said they had uncovered evidence of involvement by the Russian Business Network, a criminal gang located in St. Petersburg, but there was no clear link to the Russian military [**70**, **71**, **72**].

Georgia (2009)

Twitter service was unavailable worldwide for several hours on August 6, 2009, due to a massive DDoS attack. Max Kelly, the chief security officer at Facebook, said the attack was an effort to silence a political blogger from the Republic of Georgia, citing as evidence the fact that three other sites

used by the activist—Facebook, LiveJournal, and Google—were also targets of DDoS attacks at the same time [73, 74].

No group took responsibility for the attacks, but some noted that August 6, 2009, was the first anniversary of the war between Georgia and Russia over South Ossetia [75].

Exiled Tibetan Government (2009)

In 2009 computer security experts uncovered a surveillance effort targeting the Dalai Lama, the exiled Tibetan government, and other Tibetans. Some agencies had used backdoor Trojans to penetrate 1,295 computers in 103 countries, creating a spying system the experts named GhostNet. When a targeted person opened an email attachment supposedly containing the translation of a book, the backdoor Trojan was activated. Each backdoor Trojan was able to transfer data files and email messages back to the controlling computer. Even more ominously, it could access the computer's microphone, turning the PC into an eavesdropping station. Some of the researchers that discovered GhostNet blamed the Chinese government for the intrusions, but the Chinese government denied responsibility [76, 77].

United States and South Korea (2009)

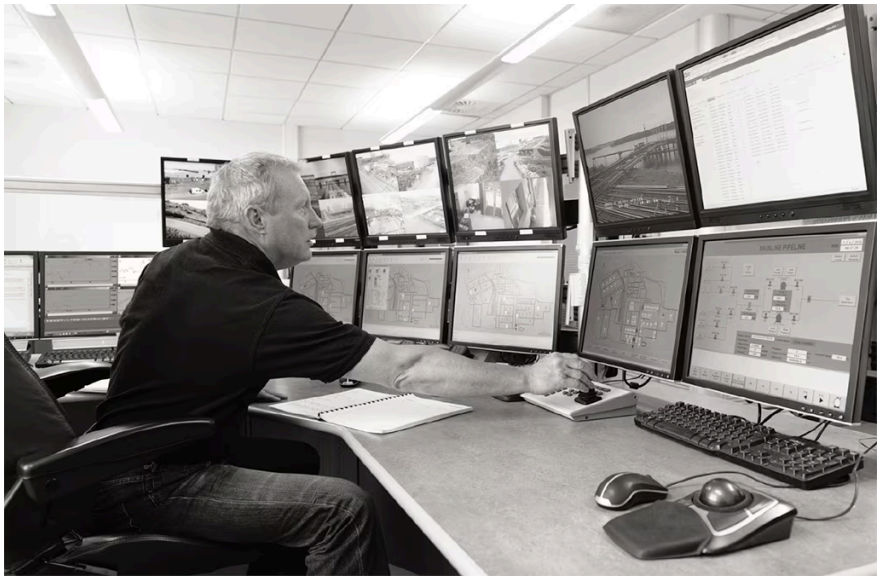
A DDoS attack on governmental agencies and commercial Web sites in the United States and South Korea paralyzed a third of them over the Fourth of July weekend in 2009. Targets in the United States included the White House, the Treasury Department, the Secret Service, the New York Stock Exchange, and NASDAQ. In South Korea, the targets included the Blue House (presidential mansion), the Defense Ministry, and the National Assembly.

The DDoS attack was relatively minor, involving a botnet containing only 50,000–65,000 computers, compared with large-scale attacks that may utilize a million computers. Still, the attack disrupted different networks over a period of days as it shifted targets, and some sites in South Korea were unavailable or compromised as late as July 9. South Korea's National Intelligence Service blamed the North Korean government or its sympathizers for the attack, hypothesizing that the attack was in retaliation for United Nations sanctions against North Korea. According to computer experts, it was unlikely the source of the attack would ever be positively identified because those responsible for the attack launched it from systems owned by others [78, 79].

Iran (2009)

Industrial processes such as chemical plants, oil and gas pipelines, and electrical power grids require constant monitoring. In the pre-computer era, monitoring was done by employees who watched gauges and warning lights, turned dials, and opened and closed valves. Computers allowed the automation of centralized monitoring. In the 1980s, distributed control systems eliminated local control cabinets. Instead, networks carried information to centralized control centers. Computer monitors with color-coded fields replaced the gauges and warning lights. Initially, distributed control systems were proprietary, but customers asked for "open systems, common protocols and vendor interoperability" [80]. They got what they wanted with the advent of supervisory control and data acquisition (SCADA) systems based on the Internet protocol. Internet-based SCADA systems are less expensive and easier to maintain and administer than proprietary systems (Figure 7.5). Another way to save money and time is to allow an outsider to connect with the SCADA system remotely to perform diagnostics.

Figure 7.5



These advances carry with them security risks. Allowing remote diagnostics creates an opportunity for a malicious outsider to gain access. Many industrial machines contain embedded microprocessors. Industrial machines last a long time, which means many of these machines contain older microprocessors. Security patches designed to ward off malware may not be available for these microprocessors, and even if they are available, it may be impractical to install them because the processor is so slow that it cannot run the security code and keep up with its machine-control responsibilities.

The Stuxnet worm, launched in 2009, attacked SCADA systems running Siemens software [81]. The worm appeared to target five industrial facilities in Iran, and it may have caused a temporary shutdown of Iran's nuclear program by infecting computers controlling centrifuges processing

uranium [82, 83]. About 1,000 of Iran's 5,000 centrifuges were damaged in the cyberattack. Developing and launching the worm was a cooperative effort between the United States and Israel [84, 85].

)

Cyber Espionage Attributed to the People's Liberation Army

American computer security firm Mandiant spent nearly a decade investigating hundreds of computer security breaches in more than a dozen countries and tracing those breaches back to the organized groups responsible for them. One of these groups, labeled APT1 (for advanced persistent threat 1), was responsible for at least 141 intrusions over a seven-year period. In 2013 Mandiant released a report stating that the APT1 group was located in Shanghai, China, and most likely was Unit 61398 of the People's Liberation Army [86].

According to Mandiant, APT1 was responsible for stealing hundreds of terabytes of data from the 141 organizations whose computer networks it compromised. One of these organizations was Telvent Canada, which provides SCADA systems to oil, gas, and electrical power companies. After Telvent Canada became aware of the security breach, it notified its customers and cut off access to their SCADA

systems from its computers in the hope of preventing a remote attack [87].

In response to the allegations made by Mandiant, Hong Lei, a spokesman for China's foreign ministry, stated that China enforces laws prohibiting cyber attacks. He continued, "Groundless criticism is irresponsible and unprofessional, and it will not help to solve the problem" [88].

In 2015 the US government disclosed that hackers had broken into computers managed by the Office of Personnel Management and had stolen the Social Security numbers and other personal information of about 22 million Americans. The stolen information included personal details provided by about 20 million Americans who had applied for security clearances. Officials fretted that this information, which included drug use and romantic histories, could provide a foreign power with an extortion tool. The prime suspect in the attack was Unit 61398 of the People's Liberation Army [89, 90].

Anonymous

The Oxford English Dictionary defines a **hacktivist** as "a computer hacker whose activity is aimed at promoting a social or political cause." Anonymous is a loosely organized

international movement of hacktivists. Individuals who identify with Anonymous are called Anons.

The profile of Anonymous was raised significantly in 2008 when it confronted the Church of Scientology [**91**]. After somebody uploaded to YouTube a video interview of Tom Cruise produced by the Church of Scientology and meant to be seen only by its members, the church filed a copyright violation claim and asked YouTube to remove it. YouTube complied with the request. In response, Anonymous issued a press release stating it was going to conduct attacks on the Church of Scientology "to end the financial exploitation of its members and protect the right to free speech" [**92**]. Anonymous members launched DDoS attacks on Scientology Web sites and worked to keep the Tom Cruise video available on the Internet. In addition, more than 6,000 Anons donned Guy Fawkes masks and protested the Church of Scientology in the streets of 90 cities across North America, Europe, Australia, and New Zealand.

Since then, a series of actions around the world have been attributed to Anonymous. Here is a sampling.

- Operation Payback was a series of DDoS attacks against the Recording Industry Association of America (RIAA), the Motion Picture Association of America

(MPAA), Indian company Aiplex, and the US Copyright Office. These attacks were launched in September 2009 after it was revealed that the RIAA and MPAA had contracted Aiplex to launch DDoS attacks on BitTorrent sites, including the Pirate Bay [**93**].

- A few months later, the focus of Operation Payback shifted to PayPal, Visa, and MasterCard after they froze the transfer of funds from supporters of Julian Assange to the WikiLeaks organization. The Web sites of all three of these financial institutions were disrupted by DDoS attacks [**94**, **95**].
- Anonymous played an active role in the Arab Spring uprisings of 2011. In Tunisia, for example, Anons launched DDoS attacks on government Web sites, offered advice to dissidents on how to conceal their identities online, and helped local activists upload videos of their protests to the Internet [**96**].
- After the US Department of Justice announced action against cybervault Mega-upload in January 2012, Anons launched DDoS attacks on the US Department of Justice, Universal Music Group, the RIAA, the MPAA, Broadcast Music Inc., and the FBI [**97**].

- Anons launched a cyber attack on Israeli Web sites on Holocaust Memorial Day in 2013 to protest Israel's treatment of Palestine [**98**].
- Anons claimed responsibility for shutting down the Web site of the City of Cleveland to protest the killing of 12-year-old Tamir Rice by a Cleveland police officer in November 2014 [**99**].
- In January 2015, after a terrorist attack on the Paris office of satirical magazine *Charlie Hebdo* left 12 dead and 11 wounded, Anonymous released a video condemning the attack and pledging to shut down jihadist Web sites [**100**].

Dozens of people around the world have been arrested for their participation in Anonymous cyber attacks, and many have spent time in prison. Dmitriy Guzner pleaded guilty to the unauthorized impairment of a protected computer in his role in the DDoS attacks against the Church of Scientology. He was sentenced to 366 days in a US federal prison and ordered to pay $37,500 in restitution [**101**]. Brian Mettenbrink was sentenced to a year in prison and ordered to pay $20,000 in restitution after pleading guilty to participating in the DDoS attacks against the Church of Scientology [**102**]. Chris Doyon was arrested for launching a

DDoS attack on a Santa Cruz County, California, Web site. He jumped bail and fled to Canada [**103**]. Briton Jake Davis pleaded guilty to participating in attacks on Sony Pictures and the Serious Organised Crime Agency in Great Britain and was given a 24-month sentence [**104**].

Ukraine

Even before Russia's invasion of Ukraine in February 2022, Ukraine was the second-most-frequent target of Russia's cyberattacks, after the United States. About a month before the invasion, the frequency of Russia's cyber attacks against Ukraine increased significantly. Microsoft observed "destructive and relentless" attacks and concluded they were designed to "disrupt or degrade Ukrainian government and military functions and undermine the public's trust in those same institutions" [**105**]. Cyber attacks focused on government computers and computers in the energy, financial, and IT sectors of the economy. Hundreds of computers were the targets of "wiper" malware that deleted data on hard drives and overwrote Master Boot Records, making the computers unbootable. Russia also initiated DDoS attacks on Ukrainian government Web sites, financial institutions, and the broadband service provider Viasat [**105**].

Summary

Computer and network security are important not just to those who manage the information-technology infrastructure of corporations and government agencies, but to anyone who has a personal computer or other devices connected to the Internet. The more that people rely upon computers and the Internet of Things, the more opportunities they provide to organizations that seek to exploit those devices to further their own aims.

Computer passwords illustrate how computer security is a trade-off between safety and convenience. Shorter passwords are easier to remember, and they take less time to enter. Unfortunately, they are easily cracked. In order to keep their systems secure, computer users must create longer, more obscure passwords that are decidedly less convenient. They should also enable multifactor authentication on their accounts.

Sometimes criminals get passwords and other sensitive information directly from computer users. Phishing attacks are an example of this kind of exploit. Some people “fall” for

phishing attacks because they are accustomed to providing sensitive information over an Internet connection.

Personal computers can become infected with malware in many different ways. Even if users remember never to open a suspect email attachment, their systems may still become infected. A worm may enter a computer by taking advantage of a security weakness in the operating system. By simply visiting a Web site, a computer user may become the target of a cross-site injection or a drive-by download. That is why it is important that all personal computer users set up personal firewalls and keep their systems up-to-date with anti-malware tools.

Criminals can also make money by co-opting personal computers and Internet-of-Things devices, turning them into bots. Bot herders rent huge botnets to those who wish to use them as launching pads for spamming, phishing attacks, or distributed denial-of-service attacks. Many Internet-connected devices, such as wireless routers, come with default administrator passwords. When consumers fail to change default passwords, they make it easy for malevolent agents to co-opt devices into botnets.

The recent rise in politically motivated cyber attacks raises some interesting questions. How vulnerable would the United

States economy be to a cyber attack by a determined foe? At what point does a cyber attack on another nation become an act of war?

Further Reading, Listening, and Viewing

Tami Abdollah and Matthew Perrone. “US Warns of Unusual Cybersecurity Flaw in Heart Devices.” Associated Press, January 11, 2017. apnews.com/dc914628d99140a391b8050e571aae05.

Tom Bearden. “Preventing a ‘Cyber-Pearl Harbor.’” *PBS NewsHour*, April 16, 2012. 7:45. video.pbs.org.

Mikko Hypponen. “Fighting Viruses, Defending the Net.” *TEDGlobal 2011*, July 2011. 17:26. www.ted.com/talks/mikko_hypponen_fighting_viruses_defendi

Brendan I. Koerner. “The Breach.” *Wired*, November 2016

James Lyne. “Everyday Cybercrime—and What You Can Do About It.” *TED*, February 2013. 17:21. www.ted.com/talks/james_lyne_everyday_cybercrime_and_wha

Annie Machon (interview). “Anonymous Ops ‘a New Front in Protest.’” *RT*, April 7, 2013. 4:18. rt.com/op-edge/.

Lily Hay Newman. “Ransomware Hits a Food Supply Giant—and Underscores a Dire Threat.” *WIRED*, June 1, 2021. https://www.wired.com/story/jbs-ransomware-attack-underscores-dire-threat/.

J.M. Porup. “Online Voting Is Impossible to Secure. So Why Are Some Governments Using It?” CSO (Web site), May 2, 2018. www.csoonline.com/article/3269297.

Avi Rubin. “All Your Devices Can Be Hacked.” *TED Talk*, February 2012. 16:56. www.ted.com/talks/.

David E. Sanger and Nicole Perlroth. “F.B.I. Identifies Group Behind Pipeline Hack.” *New York Times*, May 10, 2021. https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html.

Ray Suarez. “US Fed Up with China’s Cyber Theft, Say Analysts.” *PBS NewsHour*, July 8, 2013. 9:39. video.pbs.org.

Paul Wagenseil. “Your Router’s Security Stinks: Here’s How to Fix It.” Tom’s Guide (Web site), May 29, 2018. www.tomsguide.com/us/home-router-security,news-19245.html.

Review Questions

1. What is the common meaning of the word “hacker?”
2. Describe three “low-tech” methods that hackers have used to obtain login names and passwords.
3. Why is it dangerous to surf the Web using an open Wi-Fi network?
4. What is the difference between a computer virus and a worm?
5. What is the relationship between spyware and backdoor Trojans?
6. What is the difference between spyware and adware?
7. How are Trojan horses and drive-by downloads similar?
8. Why is it dangerous for an email program to open attachments automatically, without waiting for the user to select them?

9. Give two examples of how criminal organizations have used the Internet to make money.

10. What is a cyber attack? Give two examples of cyber attacks that have taken place outside the United States.

11. If converting SCADA systems to the Internet Protocol increases the risk of a hacker taking control of an industrial process, why are companies doing just that?

Discussion Questions

12. In a study done in London, people in subway stations were offered a cheap pen in return for disclosing their passwords. About 90 percent offered their passwords in return for the pen [**106**]. What can be done to get people to take security more seriously?

13. The default administrator password on many, if not most, home network routers never gets changed, making these computers vulnerable to malware. What would be the advantages and disadvantages of requiring the manufacturers of network routers to create a unique password for every unit they sell?

14. Email viruses are typically launched by people who modify header information to hide their identity. Brightmail's Enrique Salem says that in the future, your email reader will authenticate the sender before putting the message in your inbox. That way, you will know the source of all the emails you read. Alan Nugent of

Novell says, “I’m kind of a fan of eliminating anonymity if that is the price for security” [**107**]. Will eliminating anonymity make computers more secure?

15. Are there conditions under which the release of a worm, virus, or Trojan horse would be morally justifiable?

16. Consider a small business that is the target of a cryptographic ransomware attack. The business does not have adequate backup files, and the cost of paying the ransom is much lower than the expected cost of continuing operations without the encrypted files and recreating the necessary records. Discuss the morality of the owner choosing to pay the ransom in order to recover the business’s files.

17. When his worm program did not perform as expected, Robert Morris Jr. contacted two old friends from Harvard to decide what to do next. One of them, Andy Sudduth, agreed to email an anonymous message apologizing for the worm and describing how to protect computers from it, without disclosing Morris as the creator of the worm [**32**]. Was this the right thing for Sudduth to do?

18. Kalamazoo College requires that all computers connected to the campus network be running up-to-date antivirus software. When a student's computer is discovered to have a virus, its network connection is cut until a staff member can remove the virus. If it turns out that the computer was not running up-to-date antivirus software, the student is fined $100 [**108**]. Is this a morally justifiable policy?

19. Adam and Charlene are good friends. Both attend East Dakota State University. One day when Adam is off campus interviewing for a part-time job, someone asks him how many credit hours of computer science courses he has completed. Adam calls Charlene and asks her to access his student records by logging into the campus mainframe as if she were Adam. He provides Charlene with his student identification number and password so that she can do this. Is it wrong for Adam to share this information with Charlene? Is it wrong for Charlene to retrieve this information for Adam?

20. Carnegie Mellon University, Harvard University, and the Massachusetts Institute of Technology denied admission to more than 100 business school applicants because they took an online peek at the status of their

applications. These students learned how to circumvent the program's security, and they used this knowledge to view their files and see if they had been accepted. Students could see information about their own application, but could not view the status of other students' applications. In many cases the students learned that no admission decision had yet been made. Do you feel the response of these universities was appropriate?

21. Millions of American homes are equipped with wireless networks. If the network is not made secure, any nearby computer with a wireless card can use the network. The range of home wireless networks often extends into neighboring homes, particularly in apartment complexes. If your neighbor's wireless network extends into your home, is it wrong to use that network to get free Internet access?

22. Is it morally acceptable to use a denial-of-service attack to shut down a Web server that distributes child pornography?

23. Technological determinists argue that technological development is inevitable. If Butler had not created Firesheep, someone else would have. According to the

neutrality thesis, every invention can be put to good or bad uses. Therefore, creators of new technologies bear no moral responsibility for their inventions. In contrast, the author argues that people who create a tool making it easier for someone to do something immoral share some moral accountability for the misdeeds done by people using the tool. Which perspective do you find more compelling?

24. Do you support the actions of Anonymous? Would you consider becoming an Anon?

25. The United States and Israel cooperated to unleash the Stuxnet worm, which apparently slowed down Iran's nuclear program by damaging centrifuges processing uranium. Was unleashing the Stuxnet worm morally justifiable?

In-Class Exercises

26. The FBI obtained a court order for Apple to produce a version of iOS that would enable the FBI to unlock the cell phone of Syed Rizwan Farook and search its contents. Apple refused to comply with the court order.

    Divide the class into small groups of about four students each. Half the groups should come up with reasons why Apple should have complied with the court order. Half the groups should come up with reasons why Apple should have refused to comply with the court order. After the teams have had a reasonable amount of time to come up with their reasons, the teams should share their reasoning.

27. Debate this proposition: Those who create nondestructive malware are doing the computer industry a favor because the patches created to block them make computers more secure. To use an analogy, each virus has the effect of strengthening the immune systems of the computers it targets.

28. The University of Calgary offered a senior-level computer science course called "Computer Viruses and Malware." The course taught students how to write viruses, worms, and Trojan horses. It also discussed the history of computer viruses and taught students how to block attacks. All course assignments were done on a closed computer network isolated from the Internet. Some computer security experts criticized the university for offering the course. One researcher said, "No one argues criminology students should commit a murder to understand how a murderer thinks" [**109**]. Debate whether the University of Calgary was wrong to offer the course.

29. Debate this proposition: It is wrong for a company to hire a former malicious hacker as a security consultant.

30. A distributed denial-of-service attack makes the Web site for a top electronic retailer inaccessible for an entire day. As a result of the attack, nearly a million customers are inconvenienced, and the retailer loses millions of dollars in sales to its competitors. Law enforcement agencies apprehend the person who launched the attack. Should the punishment be determined strictly by considering the crime that was committed, or should the identity of the culprit be

taken into account? If the identity of the perpetrator should be taken into account, what punishment do you think would be appropriate if he were:

- A teenager who launched the attack out of curiosity
- An adult dedicated to fighting the country's overly materialistic culture
- A member of a terrorist organization attempting to harm the national economy

31. Divide the class into small groups of about four students. Half of the groups should come up with arguments why the United States should work to create an international ban on cyber attacks, analogous to the Chemical Weapons Convention that outlaws the production and use of chemical weapons. The other half of the groups should come up with arguments why the United States should strive to become preeminent in cyber attack technology.

References

[1] Jerry Hildenbrand. "VPNFilter Malware Has Infected a Million Routers—Here's What You Need to Know." Androidcentral (Web site), June 11, 2018. www.androidcentral.com/vpnfilter-malware.

[2] Alex Traub. "Kevin Mitnick, Once the 'Most Wanted Computer Outlaw,' Dies at 59." *New York Times*, July 20, 2023. www.nytimes.com/2023/07/20/technology/kevin-mitnick-dead-hacker.html.

[3] Dan Goodin. "Anatomy of a Hack: How Crackers Ransack Passwords Like 'qeadzwrsfxv1331.'" Ars Technica (Web site), May 27, 2013. arstechnica.com.

[4] William Cheswick. "Rethinking Passwords." *Communications of the ACM*, 52(2): 40–44, February 2013.

[5] Mat Honan. "Hacked." *Wired*, December 2012.

[6] Marcia Savage. "Mitnick Turns Gamekeeper." *TechWeb.com*, October 30, 2000.

[7] Alex Weinert. “Your Pa$$word Doesn’t Matter.” *Microsoft,* July 9, 2019. https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984.

[8] Melanie Maynes. “One Simple Action You Can Take to Prevent 99.9 Percent of Attacks on Your Accounts.” *Microsoft,* August 20, 2019. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple- action-you-can-take-to-prevent-99-9-percent-of-account-attacks/.

[9] Michael Arnone. “Hacker Steals Personal Data on Foreign Students at U. of Kansas.” *Chronicle of Higher Education*, January 24, 2003.

[10] Sara Lipka. “Hacker Breaks into Database for Tracking International Students at UNLV.” *Chronicle of Higher Education*, March 21, 2005.

[11] Dan Carnevale. “Harvard and MIT Join Carnegie Mellon in Rejecting Applicants Who Broke into Business-School Networks.” *Chronicle of Higher Education*, March 9, 2005.

[12] John P. Mello Jr. “Sesame Street Hacked, Porn Posted.” *PCWorld*, October 17, 2011.

[13] Michael S. Schmidt and Richard Péña. “F.B.I. Treating San Bernardino Attack as Terrorism Case.” *New York Times*, December 4, 2015.

[14] Government’s Motion to Compel Apple Inc. to Comply with This Court’s February 16, 2016 Order Compelling Assistance in Search. US District Court for the Central District of California. February 19, 2016. www.justice.gov/usao-cdca/file/826836/download.

[15] Tim Cook. “A Message to Our Customers.” Apple (public statement), February 16, 2016. www.apple.com/customer-letter/.

[16] “U.S. Says It Has Unlocked iPhone Without Apple.” *New York Times*, March 28, 2016. www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

[17] Ellen Nakashima. “Inspector General: FBI Didn’t Fully Explore Whether It Could Hack a Terrorist’s iPhone before Asking Court to Order Apple to Unlock It.” *Washington Post*, March 28, 2018.

[18] Eric Butler. “Firesheep.” *{codebutler}* (blog), October 24, 2010. codebutler.com.

[19] Bob Brown. “Father of Firesheep Fires Away After Wild Week in WiFi Security.” *NetworkWorld*, November 2, 2011. www.networkworld.com.

[20] Tom Anderson. “Firesheep in Wolves’ Clothing: Extension Lets You Hack into Twitter, Facebook Accounts Easily.” TechCrunch, October 24, 2010. techcrunch.com.

[21] Jason Fitzpatrick. “Firesheep Sniffs Out Facebook and Other User Credentials on Wi-Fi Hotspots.” *Lifehacker* (blog), October 25, 2010. lifehacker.com.

[22] Gregg Keizer. “How to Protect Against Firesheep Attacks.” *Computerworld*, October 26, 2010. www.computerworld.com.

[23] Sharon Machlis. “How to Hijack Facebook Using Firesheep.” *PCWorld*, October 30, 2010. www.pcworld.com.

[24] Eric Butler. “Firesheep, a Week Later: Ethics and Legality.” *{codebutler}* (blog), November 1, 2010. codebutler.com.

[25] Alex Rice. “A Continued Commitment to Security.” *The Facebook Blog*, January 26, 2011. blog.facebook.com.

[26] Paul Ducklin. “Twitter Goes Secure—Say Goodbye to Firesheep with ‘Always use HTTPS’ Option.” *nakedsecurity* (blog), March 16, 2011. nakedsecurity.sophos.com.

[27] Jessica Goodman. “Firesheep, What Color Is Your Hat?” *FeelingElephant’s Weblog*, November 30, 2010. feelingelephants.wordpress.com.

[28] David Ferbrache. *A Pathology of Computer Viruses*. Springer-Verlag, London, England, 1992.

[29] Eurostat. “Nearly One Third of Internet Users in the EU27 Caught a Computer Virus; 84% of Internet Users Use IT Security Software for Protection” (news release). February 7, 2011. europa.eu.

[30] “Google Warns TWO MILLION Users Their Computers Have Been Infected with a Virus.” *Mail Online*, July 21, 2011. www.dailymail.co.uk.

[31] John Brunner. *The Shockwave Rider*. Harper & Row, New York, NY, 1975.

[32] Katie Hafner and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon & Schuster, New York, NY, 1991.

[33] Paul Graham. "The Submarine." April 2005. www.paulgraham.com.

[34] Steve Sechrist. "State of Security: China's Trojan Horse." *Display Daily*, March 18, 2008. displaydaily.com.

[35] Roland Dela Paz. "Ransomware Attacks Continue to Spread Across Europe." Trend Micro, March 8, 2012. blog.trendmicro.com/trendlabs-security-intelligence/ransomware-attacks- continue-to-spread-across-europe/.

[36] "New Internet Scam: 'Ransomware' Locks Computers, Demands Payment." Federal Bureau of Investigation, August 9, 2012.

[37] Sean Gallagher. "FBI Says Crypto Ransomware Has Raked in > $18 Million for Cybercriminals." Ars Technica, June 25, 2015. arstechnica.com/information-technology/2015/06/fbi-says-crypto- ransomware-has-raked-in-18-million-for-cybercriminals/.

[38] Webroot. “Spyware Infection Rates Return to Peak 2004 Levels According to Webroot State of Spyware Report.” August 15, 2006. www.webroot.com.

[39] Scott Berinato. “Attack of the Bots.” *Wired*, November 2006.

[40] Cybersecurity Unit. “Securing Your ‘Internet of Things’ Devices.” US Department of Justice, July 2017. www.justice.gov/criminal-ccips/page/file/984001/download.

[41] Information Solutions Group. “Syntonic 2016 Employer Report: BYOD Usage in the Enterprise,” Syntonic Inc., Summer 2016. syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the- Enterprise.pdf.

[42] Nate Lord. “The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits.” *Digital Guardian*, February 27, 2018. digitalguardian.com/blog/ultimate-guide-byod-security-overcoming- challenges-creating-effective-policies-and-mitigating.

[43] "S. Korea Probes Cyberattack on Digital Currency Exchange." *Yonhap News Agency*, July 3, 2017. english.yonhapnews.co.kr/national/2017/07/03/52/030200000

[44] Koen van Gelder. "E-commerce Worldwide — Statistics & Facts." December 21, 2023. www.statista.com.

[45] Greg Aaron and Rod Rasmussen. "Global Phishing Survey 2H2014: Trends and Domain Name Use." APWG Internet Policy Committee, May 27, 2015. www.apwg.org.

[46] Edward Skoudis. "Evolutionary Trends in Cyberspace." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, pp. 163–164. Potomac Books, Dulles, Virginia, 2009.

[47] Lorenzo Franceschi-Bicchierai. "How Hackers Broke into John Podesta and Colin Powell's Gmail Accounts." Motherboard, October 20, 2016. motherboard.vice.com/en_us/article/mg7xjb/how-hackers-broke-into-john- podesta-and-colin-powells-gmail-accounts.

[48] Lee Fang and Naomi LaChance. "Colin Powell Urged Hillary Clinton's Team Not to Scapegoat Him for Her

Private Server, Leaked Emails Reveal." The Interceptor, September 13, 2016. theintercept.com/2016/09/13/colin-powell-emails/.

[49] CERT Coordination Center. "Denial of Service Attacks." June 4, 2001. www.cert.org/tech_tips/denial_of_service.html.

[50] Mike Toner. "Cyberterrorism Danger Lurking." *Atlanta Journal and Constitution*, November 2, 2001.

[51] Toni O'Loughlin. "Cyber Terrorism Reaches New Heights." *Australian Financial Review*, April 4, 2003.

[52] Sam Thielman and Chris Johnston. "Major Cyber Attack Disrupts Internet Service Across Europe and US." *Guardian*, October 21, 2016. www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

[53] Scott Hilton. "Dyn Analysis Summary of Friday October 21 Attack." *Dyn* (public statement), October 26, 2016. dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[54] David E. Sanger and Nicole Periroth. "A New Era of Internet Attacks Powered by Everyday Devices." *New York Times*, October 22, 2016.

www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html.

[55] "Zombie Master Jeanson Ancheta Pleads Guilty." *Spam Daily News*, January 23, 2006. www.spamdailynews.com.

[56] "Zombie Master Jeanson Ancheta Sentenced to 5 Years in Prison." *Spam Daily News*, May 9, 2006. www.spamdailynews.com.

[57] Robert Lemos. "Blue Security Folds under Spammer's Wrath." SecurityFocus (Web site), May 17, 2006. www.securityfocus.com.

[58] Kim Zetter. "TJX Hacker Charged with Heartland, Hannaford Breaches." Threat Level: Privacy, Crime and Security Online, *Wired*, August 17, 2009. www.wired.com.

[59] David Morrison. "Albert Gonzalez, Mastermind Heartland Hacker, Gets 20 Years." *Credit Union Times*, April 7, 2010. www.cutimes.com.

[60] "Avalanche Botnet Moves from Distributing Spam to Zeus Lures." *SC Magazine*, October 25, 2010. www.scmagazineuk.com.

[61] Joe Walsh. “Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline.” *Forbes,* May 8, 2021. www.forbes.com/sites/joewalsh/2021/05/08/ransomware-attack-shuts-down-massive-east-coast-gasoline-pipeline/.

[62] Natasha Bertrand, Evan Perez, Zachary Cohen, Geneva Sand s, and Josh Campbell. “Colonial Pipeline Did Pay Ransom to Hackers, Sources Now Say.” *CNN,* May 13, 2021. https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html.

[63] William Turton, Michael Riley, and Jennifer Jacobs. “Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom.” *Bloomberg,* May 13, 2021. www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom.

[64] Matt Egan. “Gas Stations in the Southeast Run Out of Gas as People Panic Buy Fuel.” *CNN,* May 12, 2021. www.cnn.com/2021/05/12/business/gas-shortage-colonial-pipeline/index.html.

[65] Christopher Bing, Joseph Menn, and Sarah N. Lynch. “U.S. Seizes $2.3 Million in Bitcoin Paid to Colonial

Pipeline Hackers." *Reuters,* June 7, 2021. www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/.

[66] Kevin O'Shea. "Cyber Attack Investigative Tools and Technologies." Institute for Security Technology Studies at Dartmouth College, May 7, 2003. www.ists.dartmouth.edu.

[67] Joshua Davis. "Hackers Take Down the Most Wired Country in Europe." *Wired*, August 21, 2007. www.wired.com.

[68] Mark Lander and John Markoff. "Digital Fears Emerge after Data Siege in Estonia." *New York Times*, May 29, 2007. www.nytimes.com.

[69] "A Look at Estonia's Cyber Attack in 2007." Associated Press, July 8, 2009. www.msnbc.msn.com.

[70] John Markoff. "Before the Gunfire, Cyberattacks." *New York Times*, August 12, 2008. www.nytimes.com.

[71] Kevin Coleman. "Cyber War 2.0—Russia v. Georgia." Defense Tech (Web site), August 13, 2008. defensetech.org.

[72] "War, Redefined." *Los Angeles Times*, August 17, 2008. articles.latimes.com.

[73] Jared Newman. "Twitter Crippled by Denial-of-Service Attack." *PCWorld Blogs*, August 6, 2009. www.pcworld.com.

[74] Elinor Mills. "Twitter, Facebook Attack Targeted One User." CNet News (Web site), August 6, 2009. news.cnet.com.

[75] Graham Cluley. "Was Twitter Denial-of-Service Targeting Anti-Russian Blogger?" *Graham Cluley's Blog*, August 7, 2009. www.sophos.com.

[76] "A Chinese Ghost in the Machine?" *Economist*, April 4, 2009.

[77] John Markoff. "Tracking Cyberspies Through the Web Wilderness." *New York Times*, May 12, 2009.

[78] Choe Sang-Hun and John Markoff. "Cyberattacks Jam Government and Commercial Web Sites in US and South Korea." *New York Times*, July 9, 2009.

[79] John Markoff. "Internet's Anonymity Makes Cyberattack Hard to Trace." *New York Times*, July 17, 2009.

[80] "Hacking the Industrial Network." Phoenix Contact Inc., Harrisburg, Pennsylvania. www.isa.org.

[81] "Siemens SCADA Systems Under Attack by Information Stealing Worm." *Help Net Security*, July 20, 2010. www.net-security.org.

[82] "Iran Confirms Stuxnet Worm Halted Centrifuges." *CBS News*, November 29, 2010. www.cbsnews.com.

[83] John Markoff. "Malware Aimed at Iran Hit Five Sites, Report Says." *New York Times*, February 11, 2011. www.nytimes.com.

[84] Christopher Williams. "Israeli Video Shows Stuxnet as One of Its Successes." *Telegraph*, February 15, 2011. www.telegraph.co.uk.

[85] David Sanger. "Obama Order Sped Up Wave of Cyberattacks against Iran." *New York Times*, June 1, 2012. www.nytimes.com.

[86] "APT1: Exposing One of China's Cyber Espionage Units." Mandiant Corporation, February 18, 2013. www.mandiant.com.

[87] David E. Sanger, David Barboza, and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *New York Times*, February 18, 2013.

[88] T.P. “Hello, Unit 61398.” *Economist*, February 19, 2013.

[89] David E. Sanger and Julie Hirschfeld Davis. “Hacking Linked to China Exposes Millions of U.S. Workers.” *New York Times*, June 4, 2015. www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html.

[90] Patricia Zengerle and Megan Cassella. “Millions More Americans Hit by Government Personnel Data Hack.” Reuters, July 9, 2015. www.reuters.com/article/us-cybersecurity-usa/millions-more-americans- hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709.

[91] Brian B. Kelly. “Investing in a Centralized Cybersecurity Infrastructure: Why ‘Hacktivism’ Can and Should Influence Cybersecurity Reform.” *Boston University Law Review*, 92(4): 1663–1711, October 2012.

[92] PRLog. “Internet Group Anonymous Declares ‘War on Scientology’” (press release). January 21, 2008. www.prlog.org.

[93] John Leyden. “4chan Launched DDoS against Entertainment Industry.” *Register*, September 20, 2010. www.theregister.co.uk.

[94] Fahmida Y. Rashid. “PayPal, PostFinance Hit by DoS Attacks, Counter-Attack in Progress.” *eWeek*, December 6, 2010. www.eweek.com.

[95] Esther Addley and Josh Halliday. “WikiLeaks Supporters Disrupt Visa and MasterCard Sites in ‘Operation Payback.’” *Guardian*, December 8, 2010. www.guardian.co.uk.

[96] Yasmine Ryan. “Anonymous and the Arab Uprisings.” Al Jazeera, May 19, 2011. www.aljazeera.com.

[97] “Internet Strikes Back: Anonymous’ Operation Megaupload Explained.” *RT*, January 20, 2012. rt.com.

[98] Adam Clark Estes. “Anonymous Hits Israel with a Massive Cyber Attack, Israel Attacks Back.” *Atlantic Wire*, April 7, 2013.

[99] David Boroff. “Grieving Dad, Anonymous Lash Out at Cleveland Cops Following Shooting Death of Boy, 12, Armed with BB Gun.” *New York Daily News*, November 24, 2014. www.nydailynews.com.

[100] Keely Lockhart. "'Hacktivist' Group Anonymous Says It Will Avenge Charlie Hebdo Attacks by Shutting Down Jihadist Websites." *Telegraph*, January 10, 2015. www.telegraph.co.uk.

[101] Nic Corbett. "Verona Teen Sentenced to Year in Prison for Online Attack of Scientology." *Star-Ledger*, New Jersey, November 18, 2009. www.nj.com.

[102] John Leyden. "Second Man Jailed over Scientology DDoS Attacks." *Register*, May 25, 2010. www.theregister.co.uk.

[103] Nate Anderson. "Anon on the Run: How Commander X Jumped Bail and Fled to Canada." Ars Technica (Web site), December 11, 2012. arstechnica.com.

[104] Dave Lee. "Jake Davis: Freed Hacker Faces Strict Tech Rules." *BBC*, June 24, 2013. www.bbc.co.uk.

[105] "An Overview of Russia's Cyberattack Activity in Ukraine." *Digital Security Unit, Microsoft,* April 27, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE

[106] John Leyden. "Office Workers Give Away Passwords for a Cheap Pen." *Register*, April 17, 2003. www.theregister.co.uk.

[107] "Fighting the Worms of Mass Destruction." *Economist*: 65–67, November 29, 2003.

[108] Kalamazoo College Information Technology Services. "Computer Virus Policy." Accessed July 29, 2011. reason.kzoo.edu.

[109] Brock Read. "How to Write a Computer Virus, for College Credit." *Chronicle of Higher Education*, 50(19): A33–A34, January 16, 2004.

Chapter 8

Computer Reliability

8.1 Introduction

ON DECEMBER 21, 2022, A SEVERE WINTER STORM IN THE UNITED STATES caused Southwest Airlines to cancel many flights. The airline's IT system was unable to cope with the high number of changes that needed to be made to the schedules of its pilots and flight attendants, and more than 16,700 flights had to be canceled between December 21 and December 31 before normal operations could result. The flight cancellations disrupted the holiday travel plans of hundreds of thousands of customers and cost the airline $800 million in lost revenues [**1**].

A computer outage affected 8,000 company-operated Starbucks stores in the United States and Canada on April 24, 2015. Some stores closed early. Others stayed open but could only accept cash for purchases. A few decided to give away free coffee or tea to appease their customers [**2**].

On August 1, 2012, Knight Capital decided to test its new software for automatic stock trades. Due to a bug in the software, it began engaging in trades where it bought stock at the (higher) asking price and immediately sold the same stock at the (lower) bidding price. In only 45 minutes, the trading

program had generated $440 million in losses for Knight Capital, driving the firm to the brink of insolvency [3].

Increasingly, we depend upon computers and computerized systems to facilitate our daily activities. They are an integral part of modern communication, transportation, retail, banking, finance, and health-care systems. When computerized systems work correctly, they save us time and money and enable us to accomplish a great deal in a day. When they fail, the benefits can turn into harms. Failures of computer-driven systems can result in lost time, lost money, and in extreme cases, injury or even death.

The purpose of this chapter is to familiarize you with various ways in which computerized systems have proven to be unreliable. Systems typically have many components, of which the computer is just one. A well engineered system can tolerate the malfunction of any single component without causing harm. Unfortunately, there are many examples of systems in which the computer or the computer-human interface was a weak link and an error led to harm. Through a variety of examples, you will gain a greater appreciation for the complexity of building a reliable computerized system.

Another important area of concern is bias exhibited by computerized decision-making systems powered by AI. We

consider a half dozen examples of algorithmic bias exhibited by deployed systems, and we explore why “fairness” can be a difficult goal for a system designer to achieve.

8.2 Data-Entry or Data-Retrieval Errors

Sometimes computerized systems fail because the wrong data have been entered into them or because people incorrectly interpret the data they retrieve. In this section, we give several examples of wrong actions being taken due to errors in data entry or data retrieval.

8.2.1 Disenfranchised Voters

In the November 2000 general election, Florida disqualified thousands of voters because preelection screening identified them as people who had been convicted of felonies. The records in the computer database, however, were incorrect; the voters had been charged with misdemeanors. Nevertheless, they were forbidden from voting. This error

may have affected the outcome of the presidential election [4].

8.2.2 False Arrests

As we saw in Chapter 6, the databases of the National Crime Information Center (NCIC) contain records related to stolen automobiles, missing persons, wanted persons, suspected terrorists, and much more. There have been numerous stories of police making false arrests based on information they retrieved from the NCIC. Here are three.

Sheila Jackson Stossier, an airline flight attendant, was arrested at the New Orleans airport by police who confused her with Shirley Jackson, who was wanted in Texas. She spent one night in jail and was detained for five days [5].

California police, relying on information from the NCIC, twice arrested and jailed Roberto Hernandez as a suspect in a Chicago burglary case. The first time he was jailed for 12 days, and the second time he was held for a week before he was freed. They had confused him with another Roberto Hernandez, who had the same height and weight. Both Hernandezes had brown hair, brown eyes, and tattoos on

their left arms. They also had the same birthday, and their Social Security numbers differed by only a single digit [**6**].

Someone used personal information about Michigan resident Terry Dean Rogan to obtain a California driver's license using his name. After the person with the falsified driver's license was arrested for two homicides and two robberies, police entered information about these crimes into the NCIC under his false identity. Over a period of 14 months, the real Terry Dean Rogan was arrested five times by Los Angeles police, three times at gunpoint, even though he and Michigan police had tried to get the NCIC records corrected after his first arrest. Rogan sued the Los Angeles Police Department and was awarded $55,000 [**5**].

8.2.3 Utilitarian Analysis: Accuracy of NCIC Records

Stepping away from a requirement of the Privacy Act of 1974, the Justice Department announced in March 2003 that it would no longer require the FBI to ensure the accuracy of information about criminals and crime victims before entering it in the NCIC database [**7**].

Should the US government take responsibility for the accuracy of the information stored in NCIC databases?

The Department of Justice argues that it is impractical for it to be responsible for the information in the NCIC database [8]: Much of the information that gets entered into the database is provided by other law enforcement and intelligence agencies. The FBI has no way of verifying that all the information is accurate, relevant, and complete. Even when the information is coming from inside the FBI, agents should be able to use their discretion to determine which information may be useful in criminal investigations. If the FBI strictly followed the provisions of the Privacy Act and verified the accuracy of every record entered into the NCIC, the amount of information in the database would be greatly curtailed. The database would be a much less useful tool for law-enforcement agencies. The result could be a decrease in the number of criminals arrested by law-enforcement agencies.

Privacy advocates counter that the accuracy of the NCIC databases is now more important than ever, because an increasing number of records are stored in these databases. As more erroneous records are put into the database, the

probability of innocent US citizens being falsely arrested also increases.

Which argument is stronger? Let's focus on one of the oldest NCIC databases: the database of stolen vehicles. The total amount of harm caused to society by automobile theft is great. Over one million automobiles are stolen in the United States every year. Victims of car theft are subjected to emotional stress, may sustain a financial loss, and can spend a lot of time trying to recover or replace the vehicle. In addition, the prevalence of automobile theft harms everyone who owns a car by raising insurance rates. In the past car thieves could reduce the probability that a stolen car would be recovered by transporting it across a state line, but the NCIC database contains information about stolen vehicles throughout the United States, and it has enabled law-enforcement officials to identify cars stolen anywhere in the nation.

At the present time, just over half of all stolen vehicles are recovered. If we make the conservative estimate that the NCIC has increased the percentage of recovered cars by just 20 percent, more than 100,000 additional cars are being returned to their owners each year. Each recovery has several benefits. First, the car is returned to its owner, who doesn't

have to go through the hassle of settling an insurance claim and getting a new vehicle. Second, by returning the car to its owner, the police make sure that "crime does not pay" and may actually apprehend a criminal, which should reduce the number of cars stolen in the future. We assign a total value of $5,000 to the benefit of returning a single stolen car to its owner. Multiplying $5,000 by 100,000, the increase in the number of cars attributed to the NCIC stolen-vehicle database, we determine the annual positive impact of the NCIC stolen-vehicle database to be $500,000,000.

Now let's consider the harmful consequences of the database. If an error in the NCIC stolen-car database leads to a false arrest, the harm caused to the innocent driver is great. However, after many years there are only a few stories of false arrests stemming from errors in the NCIC stolen-car database. Suppose there is one false arrest per year. Based on the case of Terry Dean Rogan presented earlier, we assign a total value of −$55,000 to the harm caused per false arrest.

Adding up the benefits and the harms caused by the NCIC stolen-vehicle database, we determine the operation of the database results in an annual total net increase in the happiness of the affected parties of $499,945,000. If the NCIC stolen-vehicle database did not exist, the benefit and

the harm would both be zero, meaning there would be no net increase in the happiness of the affected parties. Comparing these two alternatives, we conclude the creation and maintenance of this database has been the right course of action.

8.3 Software and Billing Errors

Even if the data entered into a computer are correct, the system may still produce the wrong result or collapse entirely if there are errors in the computer programs manipulating the data. Newspapers are full of stories about software bugs or "glitches." Here is a selection of stories that have appeared in print.

8.3.1 Errors Leading to System Malfunctions

Linda Brooks of Minneapolis, Minnesota, opened her mail on July 21, 2001, and found a phone bill for $57,346.20. A bug in Qwest's billing software caused it to charge some customers as much as $600 per minute for the use of their cell phones. About 1.4 percent of Qwest's customers, 14,000 in all, received incorrect bills. A Qwest spokesperson said the bug was in a newly installed billing system [9].

The US Department of Agriculture implemented new livestock price-reporting guidelines after discovering that software errors had caused the USDA to understate the prices meatpackers were receiving for beef. Since beef producers and packers negotiate cattle contracts based on the USDA price reports, the errors cost beef producers between $15 and $20 million [**10**].

In 1996 a software error at the US Postal Service resulted in two weeks' worth of mail addressed to the Patent and Trademark Office being returned to the senders. In all, 50,000 pieces of mail were returned [**11**].

Between September 2008 and May 2009, hundreds of families living in public housing in New York City were charged too much rent because of an error in the program that calculated their monthly bills. For nine months, the New York City Housing Authority did not take seriously the renters' complaints that they were being overcharged. Instead, it took to court many of the renters who did not make the higher payments and threatened them with eviction [**12**].

In California in 2010 about 450 people who were incarcerated and characterized as exhibiting a "high risk of

violence" were mistakenly released as part of a program meant to reduce prison overcrowding. California officials could not return any of them to prison or put them on supervised parole because they had already been granted "nonrevocable parole" [**13**].

8.3.2 Errors Leading to System Failures

On the first day that a new, fully computerized ambulance dispatch system became operational in the city of London, people making emergency calls were put on hold for up to 30 minutes, with the system losing track of some calls, and ambulances took up to three hours to respond. As many as 20 people died because ambulances did not arrive in time [**14**].

Japan's air traffic control system went down for an hour on the morning of March 1, 2003, delaying departures for hours. The backup system failed at the same time as the main system, which was out of commission for four hours. Airports kept in touch via telephone, and no passengers were put at risk. However, some flights were delayed over two hours, and 32 domestic flights had to be canceled [**15**].

A new laboratory computer system at Los Angeles County+USC Medical Center became backlogged the day after it was turned on. For several hours on both April 16 and April 17, 2003, emergency room doctors told the County of Los Angeles to stop sending ambulances, because the doctors could not get access to the laboratory results they needed. “It’s almost like practicing Third World medicine,” said Dr. Amanda Garner. “We rely so much on our computers and our first-world technology that we were almost blinded” [**16**].

In August 2005, the passengers on a Malaysia Airlines flight from Perth, Australia, to Kuala Lumpur, Malaysia, suddenly found themselves on a roller-coaster–like ride seven miles above the Indian Ocean. When the Boeing 777 unexpectedly began a rapid climb, the pilot disconnected the autopilot, but it took him 45 seconds to regain control of the jet. The plane zoomed upward, downward, and then upward a second time before leveling out. After an investigation, Boeing reported that a software error had caused the flight computers to receive faulty information about the plane’s speed and acceleration. In addition, another error had caused the flight computers to fail to respond immediately to the pilot’s commands [**17**].

A software problem forced the NASDAQ stock exchange to shut down for three hours in 2013. Two years later, the New York Stock Exchange halted trading for nearly four hours because of a computer-related "configuration problem" [**18**, **19**].

At the Black Hat conference in Las Vegas in 2011, computer security researcher Jay Radcliffe demonstrated how he could wirelessly hack into and control the insulin pump he was wearing, giving him the ability to change the amount of insulin it was dispensing. According to Radcliffe, the only information a hacker would need to take control of a particular pump is the pump's serial number [**20**].

In July 2015, two researchers demonstrated to a journalist how they could hack wirelessly into a Jeep Cherokee equipped with a touch screen and Uconnect software and gain control of the vehicle's vital systems. As the journalist, who had consented to the experiment, drove a Cherokee around St. Louis, the hackers, sitting at a laptop computer 10 miles away, took control of the SUV's climate control system, radio, windshield wipers, transmission, and brakes [**21**]. All Chrysler vehicles from model years 2013 through 2015 equipped with touch screens and Uconnect software had the security vulnerability. National Highway Traffic Safety

Administration officials insisted that Fiat Chrysler announce a formal safety recall of 1.4 million affected vehicles to highlight to owners the importance of installing a software patch [22].

8.3.3 Analysis: E-Retailer Posts Wrong Price, Refuses to Deliver

Amazon.com shut down its British Web site on March 19, 2003, after a software error led it to offer iPAQ handheld computers for 7 pounds instead of the correct price of about 275 pounds. Before Amazon.com shut down the site, electronic bargain hunters had flocked to Amazon.com's Web site, some of them ordering as many as 10 iPAQs [23]. Amazon said that customers who ordered at the mistaken price should not expect delivery unless they paid the difference between the advertised price and the actual price. An Amazon.com spokesperson said, "In our Pricing and Availability Policy, we state that where an item's correct price is higher than our stated price, we contact the customer before dispatching. Customers will be offered the opportunity

either to cancel their order or to place new orders for the item at the correct price" [**24**].

Was Amazon.com wrong to refuse to fill the orders of the people who bought iPAQs for 7 pounds?

Let's analyze the problem from a rule-utilitarian point of view. We can imagine a moral rule of the form, "A person or organization wishing to sell a product must always honor the advertised price." What would happen if this rule were universally followed? More time and effort would be spent proofreading advertisements, whether printed or electronic. Organizations responsible for publishing the advertisements in newspapers, magazines, and Web sites would also take more care to ensure no errors were introduced. There is a good chance companies would take out insurance policies to guard against the catastrophic losses that could result from a typo. To pay for these additional costs, the prices of the products sold by these companies would be higher. The proposed rule would harm every consumer who ended up paying more for products. The rule would benefit the few consumers who took advantage of misprints to get good deals on certain goods. We conclude the proposed moral rule has more harms than benefits, and Amazon.com did the right thing by refusing to ship the iPAQs.

We *could* argue, from a Kantian point of view, that the knowledgeable consumers who ordered the iPAQs did something wrong. The correct price was 275 pounds; the advertised price was 7 pounds. While electronic products may go on sale, retailers simply do not drop the price of their goods by 97.5 percent, even when they are being put on clearance. If consumers understood the advertised price was an error, then they were taking advantage of Amazon.com's stockholders by ordering the iPAQ before the error was corrected. They were not acting "in good faith."

8.4 Notable Software System Failures

In this section we shift our focus to complicated devices or systems controlled at least in part by computers. An **embedded system** is a computer used as a component of a larger system. You can find microprocessor-based embedded systems in microwave ovens, thermostats, automobiles, traffic lights, and a myriad of other modern devices. Because computers need software to execute, every embedded system has a software component.

Software is playing an ever-larger role in system functionality [25]. There are several reasons why hardware controllers are being replaced by microprocessors controlled by software. Software controllers are faster. They can perform more sophisticated functions, taking more input data into account. They cost less, use less energy, and do not wear out. Unfortunately, while hardware controllers have a reputation

for high reliability, the same cannot be said for their software replacements.

Most embedded systems are also **real-time systems:** computers that process data from sensors as events occur. The microprocessor that controls the air bags in a modern automobile is a real-time system, because it must instantly react to readings from its sensors and deploy the air bags at the time of a collision. The microprocessor in a cell phone is another example of a real-time system that converts electrical signals into radio waves and vice versa.

This section contains seven examples of computer system failures: the Patriot missile system used in the Gulf War, the Ariane 5 launch vehicle, AT&T's long-distance network, NASA's robot missions to Mars, the automated baggage system at Denver International Airport, the Tokyo Stock Exchange, and direct-recording electronic voting machines. These are all examples of embedded, real-time systems. In every case at least part of the failure was due to errors in the software component of the system. Studying these errors provides important lessons for anyone involved in the development of an embedded system.

8.4.1 Patriot Missile

The Patriot missile system was originally designed by the US Army to shoot down airplanes. In the 1991 Gulf War, the Army put the Patriot missile system to work defending against Scud missiles launched at Israel and Saudi Arabia.

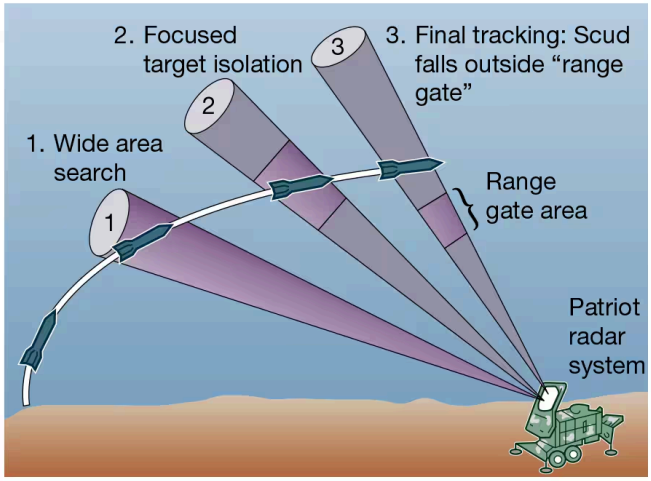
At the end of the Gulf War, the Army claimed the Patriot missile defense system had been 95 percent effective at destroying incoming Scud missiles. Later analyses showed that perhaps as few as 9 percent of the Scuds were actually destroyed by Patriot missiles. As it turns out, many Scuds simply fell apart as they approached their targets—their destruction had nothing at all to do with the Patriot missiles launched at them.

The most significant failure of the Patriot missile system occurred during the night of February 25, 1991, when a Scud missile fired from Iraq hit a US Army barracks in Dhahran, Saudi Arabia, killing 28 soldiers. The Patriot missile battery defending the area never even fired at the incoming Scud.

Mississippi congressman Howard Wolpe asked the General Accounting Office (GAO) to investigate this incident. The GAO report traced the failure of the Patriot system to a software error (Figure 8.1). The missile battery did detect the incoming Scud missile as it came over the horizon. However,

in order to prevent the system from responding to false alarms, the computer was programmed to check multiple times for the presence of the missile. The computer predicted the flight path of the incoming missile, directed the radar to focus in on that area, and scanned a segment of the radar signal, called a range gate, for the target. In this case the program scanned the wrong range gate. Since it did not detect the Scud, it did not fire the Patriot missile.

Figure 8.1



A software error caused the Patriot missile system to lose track of incoming Scud missiles. (1) The radar system doing a wide area search picks up the Scud missile. (2) The radar system isolates the proposed target. (3) A software error causes the system to produce a faulty range gate. The system loses track of the missile, because it does not fly through this gate.

(Eliot Marshall, "Fatal Error: How Patriot Overlooked a Scud," Vol 255(5050), 13 Mar 1992. Used with permission from AAAS.)

Why did the program scan the wrong range gate? The tracking system relied upon getting signals from the system

clock. These values were stored in a floating-point variable with insufficient precision, resulting in a small mathematical error called a *truncation*. The longer the system ran, the more these truncation errors added up. The Patriot missile system was designed to operate for only a few hours at a time. However, the system at Dhahran had been in continuous operation for 100 hours. The accumulation of errors led to a difference between the actual time and the computed time of about 0.3433 seconds. Because missiles travel at high speeds, the 0.3433-second error led to a tracking error of 687 meters (about half a mile). That was enough of an error to prevent the missile battery from locating the Scud in the range gate area [**26**].

)

8.4.2 Ariane 5

The Ariane 5 was a satellite launch vehicle designed by the French space agency, the Centre National d'Etudes Spatiales, and the European Space Agency. About 40 seconds into its maiden flight on June 4, 1996, a software error caused the nozzles on the solid boosters and the main rocket engine to swivel to extreme positions. As a result, the rocket veered sharply off course. When the links between the solid boosters and the core stage ruptured, the launch vehicle self-

destructed. The rocket carried satellites worth $500 million, which were not insured [27].

A board of inquiry traced the software error to a piece of code that converts a 64-bit floating-point value into a 16-bit signed integer. The value to be converted exceeded the maximum value that could be stored in the integer variable, causing an exception to be raised. Unfortunately, there was no exception-handling mechanism for this particular exception, so the onboard computers crashed.

The faulty piece of code had been part of the software for the Ariane 4. The 64-bit floating-point value represented the horizontal bias of the launch vehicle, which is related to its horizontal velocity. When the software module was designed, engineers determined that it would be impossible for the horizontal bias to be so large that it could not be stored in a 16-bit signed integer. There was no need for an error handler, because an error could not occur. This code was moved "as is" into the software for the Ariane 5. That proved to be an extremely costly mistake, because the Ariane 5 was faster than the Ariane 4. The original assumptions made by the designers of the software no longer held true [28].

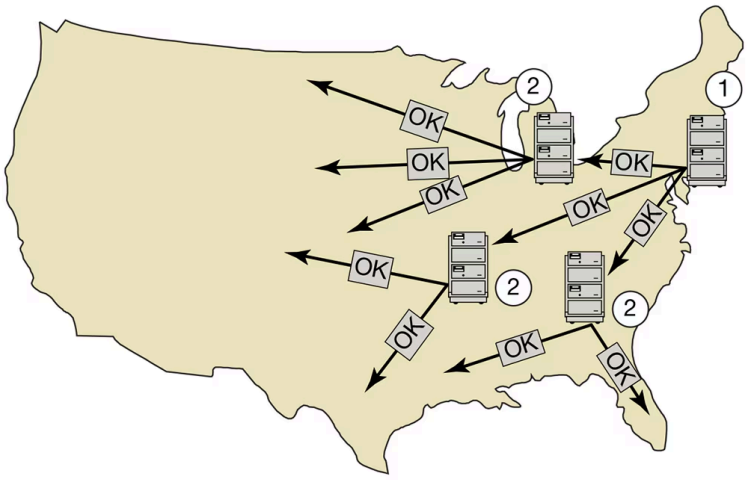
8.4.3 AT&T Long-Distance Network

On the afternoon of January 15, 1990, AT&T's long-distance network suffered a significant disruption of service. About half of the computerized telephone routing switches crashed, and the remainder of the switches could not handle all the traffic. As a result of this failure, about 70 million long-distance telephone calls could not be put through, and about 60,000 people lost all telephone service. AT&T lost tens of millions of dollars in revenue. It also lost some of its credibility as a reliable provider of long-distance service.

Investigation by AT&T engineers revealed that the network crash was brought about by a single faulty line of code in an error-recovery procedure. The system was designed so that if a server discovered it was in an error state, it would reboot itself, a crude but effective way of "wiping the slate clean." After a switch rebooted itself, it would send an "OK" message to other switches, letting them know it was back online. The software bug manifested itself when a very busy switch received an "OK" message. Under certain circumstances, handling the "OK" message would cause the busy switch to enter an error state and reboot.

On the afternoon of January 15, 1990, a switch in New York City using the company's new System 7 software detected an error condition and rebooted itself (Figure 8.2). When it came back online, it broadcast an "OK" message. All the switches receiving the "OK" messages handled them correctly, except three very busy switches in St. Louis, Detroit, and Atlanta. These switches detected an error condition and rebooted. When they came back up, all of them broadcast "OK" messages across the network, causing other switches to fail in an ever-expanding wave.

Figure 8.2



A software bug in error recovery code made AT&T's System 7 switches crash in 1990. (1) A single switch in New York City detects an error condition and reboots. When it comes back up, it sends an "OK" message to other switches. (2) Switches in Detroit, St. Louis, and Atlanta are so busy that handling the "OK" message causes them to fail. They detect an error condition and reboot. When they come back up, they send out "OK" messages to other switches, causing some of them to fail, and so on.

Every switch failure compounded the problem in two ways. When the switch went down, it pushed more long-distance traffic onto the other switches, making them busier. When the switch came back up, it broadcast "OK" messages to these busier switches, causing some of them to fail. Some switches rebooted repeatedly under the barrage of "OK" messages. Within 10 minutes, half the switches in the AT&T network had failed.

The crash could have been much worse, but AT&T had converted only 80 of its network switches to the System 7 software. It had left System 6 software running on 34 of the switches "just in case." The System 6 switches did not have the software bug and did not crash [**29, 30**].

8.4.4 Robot Missions to Mars

NASA designed the $125 million Mars Climate Orbiter to facilitate communications between Earth and automated probes on the surface of Mars, including the Mars Polar Lander. Ironically, the spacecraft was lost because of a miscommunication between two support teams on Earth.

The Lockheed Martin flight operations team in Colorado designed its software to use English units. Its program output thrust in terms of foot-pounds. The navigation team at the Jet Propulsion Laboratory in California designed its software to use metric units. Its program expected thrust to be input in terms of newtons. One foot-pound equals 4.45 newtons. On September 23, 1999, the Mars Climate Orbiter neared the Red Planet. When it was time for the spacecraft to fire its engine to enter orbit, the Colorado team supplied thrust information to the California team, which relayed it to the spacecraft. Because of the units mismatch, the navigation team specified 4.45 times too much thrust. The spacecraft flew too close to the surface of Mars and burned up in its atmosphere.

A few months later NASA's Martian program suffered a second catastrophe. The Mars Polar Lander, produced at a cost of $165 million, was supposed to land on the south pole of Mars and provide data that would help scientists understand how the Martian climate has changed over time. On December 3, 1999, NASA lost contact with the Mars Polar Lander. NASA engineers suspect that the system's software got a false signal from the landing gear and shut down the engines 100 feet above the planet's surface.

Tony Spear was project manager of the Mars Pathfinder mission. He said, “It is just as hard to do Mars missions now as it was in the mid-’70s. I’m a big believer that software hasn’t gone anywhere. Software is the number one problem” [**31**].

Several years after Spear made this observation, NASA successfully landed two Mars Exploration Rovers on the Red Planet [**32**]. The rovers, named Opportunity and Spirit, were launched from Earth in June and July of 2003, successfully landing on Mars in January 2004. Mission planners had hoped that each rover would complete a three-month mission, looking for clues that the Martian surface once had enough water to sustain life. The rovers greatly exceeded this goal. The Spirit rover operated successfully for more than five years. Opportunity found evidence of a former saltwater lake and operated for 14 years and 138 days.

8.4.5 Denver International Airport

As airline passenger traffic strained the capacity of Stapleton International Airport, the City and County of Denver planned the construction of a much larger airport. Stapleton

International Airport had earned a reputation for slow baggage handling, and the project planners wanted to ensure the new airport would not suffer from the same problem. They announced an ambitious plan to create a one-of-a-kind, state-of-the-art automated baggage-handling system for the Denver International Airport (DIA).

The airport authorities signed a $193 million contract with BAE Automated Systems to design and build the automated baggage-handling system, which consisted of thousands of baggage carts traveling roller-coaster–style on 21 miles of metal tracks. According to the design, agents would label a piece of luggage and put it on a conveyor belt. Computers would route each bag along one or more belts until it reached a cart-loading point, where each bag would be loaded into its own tublike cart. Scanners would read the destination information from the suitcase label, and computers would then route each cart along the tracks at 20 miles per hour to the correct unloading point, where each bag would be unloaded onto a conveyor belt and carried to its final destination. To monitor the movement of the bags, the system used 56 bar-code scanners and 5,000 electric eyes.

There were problems from the outset of the project. The airport design was already completed before the baggage-

handling system was chosen. As a result, the underground tunnels were small and had sharp turns, making it difficult to shoehorn in an automated baggage system. And given its ambitious goals, the project timeline was too short.

However, the most important problem with the automated baggage handler was that the complexity of the system exceeded the ability of the development team to understand it. Here are a few of the problems BAE encountered.

- Luggage carts were misrouted and failed to arrive at their destinations.
- Computers lost track of where the carts were.
- Bar-code printers didn't print tags clearly enough to be read by scanners.
- Luggage had to be correctly positioned on conveyors in order to load properly.
- Bumpers on the carts interfered with the electric photocells.
- Workers painted over electric eyes or knocked photo sensors out of alignment.
- Light luggage was thrown off rapidly moving carts.

- Luggage was shredded by automated baggage handlers.
- The design did not consider the problem of fairly balancing the number of available carts among all the locations needing them.

BAE attempted to solve these problems one at a time by trial and error, but the system was too complicated to yield to that kind of problem-solving approach. BAE should have been looking at the big picture, trying to find where the specifications for the system were wrong or unattainable.

DIA was supposed to open on October 31, 1993. The opening was delayed repeatedly because the baggage-handling system was not yet operational. Eventually, the mayor of Denver announced the city would spend $50 million to build a conventional luggage-handling system using tugs and carts. (This conventional system actually ended up costing $71 million.) On February 28, 1995, flights to and from the new airport began. However, concourse A was not open at all. Concourse C opened with 11 airlines using a traditional baggage system. The BAE automated system, far over budget at $311 million, was used only by United Airlines in concourse B to handle outgoing baggage originating in Denver. United Airlines used a traditional system for the rest of its baggage in concourse B.

The failure of BAE to deliver a working system on time resulted in a 16-month delay in the opening of DIA. This delay cost Denver $1 million *a day* in interest on bonds and operating costs. As a result, DIA began charging all the airlines a flight fee of about $20 per passenger, the highest airport fee in the nation. Airlines passed along this cost to consumers by raising ticket prices of flights going through Denver [33].

8.4.6 Tokyo Stock Exchange

December 8, 2005, was the first day that shares of J-Com, a recruiting company, were made available to the public on the Tokyo Stock Exchange. That morning, an employee of Mizuho Securities received a call from a customer who said he wished to sell one share of J-Com stock at a price of 610,000 yen. At 9:27 a.m., the Mizuho Securities employee mistakenly entered an order to sell 610,000 shares of J-Com at 1 yen per share. When the computer screen displayed a "Beyond price limit" warning, the employee overrode the warning by hitting the Enter key twice, sending the order to the Tokyo Stock Exchange. At 9:28 a.m., the sell order appeared on the Tokyo Stock Exchange's display board. Spotting the mistake, Mizuho Securities attempted to cancel

the sell order several times between 9:29 and 9:35 a.m., but these attempts failed because of a bug in the Tokyo Stock Exchange trading program. Mizuho also phoned the Tokyo Stock Exchange, asking the TSE to cancel the sell order, but the Tokyo Stock Exchange refused.

Beginning at 9:35 a.m., Mizuho started to buy back shares of J-Com, but it was only able to purchase about a half million shares. More than 96,000 shares had already been purchased by other parties. It was impossible for Mizuho to provide shares to these buyers because J-Com only had 14,500 publicly traded shares. Under the terms of a special arrangement brokered by the stock exchange, Mizuho settled these accounts by paying 912,000 yen per share to the buyers. In all, Mizuho Securities lost 40 billion yen ($225 million) buying back shares. When the Tokyo Stock Exchange refused to compensate Mizuho Securities for the loss, Mizuho Securities sued the Tokyo Stock Exchange for $416 million. A court ruled in favor of Mizuho Securities but reduced the compensation from the Tokyo Stock Exchange to $107 million because it was the error of a Mizuho Securities employee that caused the problem in the first place [**34**].

Eventually, the Tokyo Stock Exchange identified the bug that prevented the order from being canceled. The bug had gone

undetected for five years because it only occurred when seven different unusual conditions all happened simultaneously [35].

8.4.7 Direct-Recording Electronic Voting Machines

Nearly two million ballots were not counted in the 2000 US presidential election because they registered either no choice or multiple choices. The incredibly close election in Florida was marred by voting-machine controversies. To avoid a repeat of these problems, Congress passed, and President Bush signed, the Help America Vote Act of 2002 (HAVA). HAVA provided money to states to replace punch-card voting systems and improve standards for administering elections [36].

Many states used HAVA funds to purchase direct-recording electronic (DRE) voting machines. DRE voting machines allow voters to indicate each of their choices by touching the screen or pressing a button (Figure 8.3). After all selections have been made, a summary screen displays the voter's choices. At this point, the voter may either cast the ballot or back up to make changes.

Figure 8.3

This Diebold voting machine uses a touch-sensitive screen to capture each voter's choices.

(Rogelio Solis/AP Images)

Brazil and India have run national elections using DRE voting machines exclusively [37]. By the time of the November 2006 general election, about one-third of US voters cast their ballots on DRE systems. Proponents of DRE voting machines pointed out the speed and accuracy of machine counting. They said the systems were more tamper-resistant than paper ballots, which can be marked by election

workers. When the ballots are electronic, it is impossible for precincts to run out of ballots if turnout is higher than expected. In addition, touch-screen voting machines can be programmed to help voters avoid the errors of not choosing a candidate or selecting too many candidates [38].

Some computer experts spoke out against the conversion to touch-screen voting machines, arguing that they are not necessarily any better than the systems they are replacing. In particular, experts expressed concerns about programming errors and the lack of a **paper audit trail**: a record of the original ballots cast.

Quite a few voting irregularities were linked to DRE voting machines since 2002. Here is a selection.

- In November 2002, a programming error caused a touch-screen voting machine to fail to record 436 ballots cast in Wake County, North Carolina [39].
- Touch-screen voting machines reported that 144,000 ballots were cast in a 2003 election held in Boone County, Indiana, even though the county had only 19,000 registered voters. After a programming error was fixed, the ballots were recounted, producing new results consistent with the number of votes actually

cast. However, because there was no paper audit trail, there was no way to know if the new results were correct [**40**].

- Florida held a special election in January 2004 to determine who would represent State House District 91. When the 10,844 votes were tallied, the voting machines reported that 134 voters had not voted for a candidate, even though that was the only race on the ballot. The winning candidate received 12 more votes than the runner-up. Since the voting machines had no record of the original votes, there was no recount [**40**].
- In November 2004, initial printouts from all the DRE voting machines in LaPorte County, Indiana, reported exactly 300 votes, disregarding more than 50,000 votes until the problem was sorted out [**41**].
- In November 2004, a bug in the vote-counting software in DRE voting machines in Guilford County, North Carolina, caused the systems to begin counting backward after they reached a maximum count of 32,767. After the problem was fixed, a recount changed the outcome of two races and gave another 22,000 votes to presidential candidate John Kerry [**42**].

- In 2006 some Florida voters had a hard time voting for Democratic candidates on DRE voting machines. After choosing Democrats, these voters discovered that the machine's summary screen replaced some of the Democrats with their Republican opponents. Some voters had to repeat their votes several times in order for the proper candidate's name to appear on the summary screen [**43**].
- In a congressional election held in November 2006 in Florida, more than 18,000 votes cast on DRE voting machines were not recorded. The final tally showed Republican Vern Buchanan beating Democrat Christine Jennings by only 369 votes [**44**].

Some computer experts expressed concerns about the vulnerability of electronic voting machines to tampering. Finnish security specialist Harri Hursti investigated the memory cartridges used to record votes in Diebold DRE voting machines. (After the polls close, these cartridges are removed from the machines and taken to a central location, where the votes are tallied.) Hursti discovered that he could use a readily available agricultural scanning device to change the vote counts without leaving a trace [**45**].

Computer science professor Herbert Thompson examined the centralized Diebold machine that tallies the votes from the individual DRE voting machines. According to Thompson, the system lacked even a rudimentary authentication mechanism; he was able to access the system's program without a login name or password. By inserting just five lines of code, he successfully switched 5,000 votes from one candidate to another. "I am positive an eighth grader could do this," he said [**45**].

The AVS WinVote DRE system was adopted in Mississippi, Pennsylvania, and Virginia, though after 2008 Virginia was the only state to use WinVote machines. Unlike other DRE systems, the WinVote system used Wi-Fi to simplify setting up voting machines and counting the votes from the many machines at a single precinct. An assessment by the Virginia Information Technology Agency (VITA) revealed that WinVote had a number of serious security weaknesses. In particular, the system used obsolete WEP wireless encryption, had a hardwired WEP key of "abcde," used another hardwired key to encrypt the database, and lacked "logs or checksums to detect whether the database had been replaced" [**46**]. VITA determined that it would be possible for someone to modify the results of an election by taking the following steps: capturing the wireless traffic between the voting

machines; breaking the WEP encryption; connecting to the machines; downloading the Microsoft Access databases containing the votes; modifying the databases to add, change, or delete votes; and uploading the modified databases to the voting machines. After receiving this information, the Virginia State Board of Elections decertified the WinVote machines [**46**].

Without access to the source code to touch-screen systems, there is no way to test how secure they are. The manufacturers of these systems refused to make the software public, saying the source code is valuable intellectual property—a trade secret. The Open Voting Consortium criticized the corporate control of elections in the United States and advocated the development of open-source software to make elections "open and transparent" [**47**].

Critics of touch-screen voting systems claimed these systems make possible an unprecedented level of election fraud. The old, lever-style mechanical voting machines were susceptible to fraud at the local level. A voting official could enter a voting booth and vote multiple times for a slate of candidates, but the number of extra votes that could be added in any precinct without attracting attention was limited. In contrast, by changing the programming of an

electronic voting system, a single person could change votes across thousands of precincts [48].

Supporters of touch-screen voting machines said criticisms of DRE voting machines were overblown. A report by the Pacific Research Institute maintained that DRE voting systems are more secure than traditional paper ballots, which can be tampered with by elections officials. “Open source advocates and paper trail champions want to steer e-voting off a cliff. Rather than demanding utopian machines and spreading conspiracy theories for political gain, they should refocus their energy in a way that actually helps American voters” [49].

The arguments of the DRE machine skeptics have prevailed in the United States. Most states have turned away from DRE voting machines. In the 2022 midterm elections, 70 percent of US voters cast their votes with paper ballots. In most cases, these paper ballots were automatically counted using an electronic scanner. Another 23 percent of US voters cast their ballots with machines that produce a paper record of the voter’s choices. Only 7 percent of US voters used DRE machines [50].

8.5 Therac-25

Soon after German physicist Wilhelm Roentgen discovered the X-ray in 1895, physicians began using radiation to treat cancer. Today, between 50 and 60 percent of cancer patients are treated with radiation, either to destroy cancer cells or relieve pain. Linear accelerators create high-energy electron beams to treat shallow tumors and X-ray beams to reach deeper tumors.

The Therac-25 linear accelerator was notoriously unreliable. It was not unusual for the system to malfunction 40 times a day. We devote an entire section to telling the story of the Therac-25 because it is a striking example of the harm that can be caused when the safety of a system relies solely upon the quality of its embedded software.

In a 20-month period between June 1985 and January 1987, the Therac-25 administered massive overdoses to six patients, causing the deaths of three of them. While 1987 may seem like the distant past, it does give us the advantage of 20/20 hindsight. The entire story has been thoroughly researched and documented [**51**]. Failures of computerized systems

continue to this day, but none have been analyzed as thoroughly as the Therac-25 failure.

8.5.1 Genesis of the Therac-25

Atomic Energy of Canada Limited (AECL) and the French corporation CGR cooperated in the 1970s to build two linear accelerators: the Therac-6 and the Therac-20. Both the Therac-6 and the Therac-20 were modernizations of older CGR linear accelerators. The distinguishing feature of the Therac series was the use of a DEC PDP 11 minicomputer as a "front end." By adding the computer, the linear accelerators were easier to operate. The Therac-6 and the Therac-20 were actually capable of working independently of the PDP 11, and all of their safety features were built into the hardware.

After producing the Therac-20, AECL and CGR went their separate ways. AECL moved ahead with the development and deployment of a next-generation linear accelerator called the Therac-25. Like the Therac-6 and the Therac-20, the Therac-25 made use of a PDP 11. Unlike its predecessor machines, however, AECL designed the PDP 11 to be an integral part of the device; the linear accelerator was

incapable of operating without the computer. This design decision enabled AECL to reduce costs by replacing some of the hardware safety features of the Therac-20 with software safety features in the Therac-25.

AECL also decided to reuse some of the Therac-6 and Therac-20 software in the Therac-25. Code reuse saves time and money. Theoretically, “tried-and-true” software is more reliable than newly written code, but as we shall see, that assumption was invalid in this case.

AECL shipped its first Therac-25 in 1983. In all, it delivered 11 systems in Canada and the United States. The Therac-25 was a large machine that was placed in its own room. Shielding in the walls, ceiling, and floor of the room prevented outsiders from being exposed to radiation. A television camera, microphone, and speaker in the room allowed the technician in an adjoining room to view and communicate with the patient undergoing treatment.

8.5.2 Chronology of Accidents and AECL Responses

We now chronicle six major incidents involving the Therac-25 that occurred between June 1985 and January 1987, along with the AECL responses to them.

Marietta, Georgia, June 1985

A 61-year-old patient with breast cancer was being treated at the Kennestone Regional Oncology Center. After radiation was administered to the area of her collarbone, she complained that she had been burned.

The Kennestone physicist contacted AECL and asked if it was possible that the Therac-25 had failed to diffuse the electron beam. Engineers at AECL replied that this could not happen.

The patient suffered crippling injuries as a result of the overdose, which the physicist later estimated was 75 to 100 times too large. She sued AECL and the hospital in October 1985.

Hamilton, Ontario, July 1985

A 40-year-old woman was being treated for cervical cancer at the Ontario Cancer Foundation. When the operator tried to administer the treatment, the machine shut down after five seconds with an error message. According to the display, the linear accelerator had not yet delivered any radiation to the

patient. Following standard operating procedure, the operator typed “P” for “proceed.” The system shut down in the same way, indicating that the patient had not yet received a dose of radiation. (Recall it was not unusual for the machine to malfunction several dozen times a day.) The operator typed “P” three more times, always with the same result, until the system entered “treatment suspend” mode.

The operator went into the room where the patient was. The patient complained that she had been burned. The lab called in a service technician, who could find nothing wrong with the machine. The clinic reported the malfunction to AECL.

When the patient returned for further treatment three days later, she was hospitalized for a radiation overdose. It was later estimated that she had received between 65 and 85 times the normal dose of radiation. The patient died of cancer in November 1985.

First AECL Investigation, July–September 1985

After the Ontario overdose, AECL sent out an engineer to investigate. While the engineer was unable to reproduce the overdose, he did uncover design problems related to a

microswitch. AECL introduced hardware and software changes to fix the microswitch problem.

Yakima, Washington, December 1985

The next documented overdose accident occurred at Yakima Valley Memorial Hospital. A woman receiving a series of radiation treatments developed a strange reddening on her hip after one of the treatments. The inflammation took the form of several parallel stripes. The hospital staff tried to determine the cause of the unusual stripes. They suspected the pattern could have been caused by the slots in the accelerator's blocking trays, but these trays had already been discarded by the time the staff began their investigation. After ruling out other possible causes for the reaction, the staff suspected a radiation overdose and contacted AECL by letter and by phone.

AECL replied in a letter that neither the Therac-25 nor operator error could have produced the described damage. Two pages of the letter explained why it was technically impossible for the Therac-25 to produce an overdose. The letter also claimed that no similar accidents had been reported.

The patient survived, although the overdose scarred her and left her with a mild disability.

)

Tyler, Texas, March 1986

A male patient came to the East Texas Cancer Center (ETCC) for the ninth in a series of radiation treatments for a cancerous tumor on his back. The operator entered the treatment data into the computer. She noticed that she had typed “X” (for X-ray) instead of “E” (for electron beam). This was a common mistake, because X-ray treatments are much more common. Being an experienced operator, she quickly fixed her mistake by using the up arrow key to move the cursor back to the appropriate field, changing the “X” to an “E” and moving the cursor back to the bottom of the screen. When the system displayed “beam ready,” she typed “B” (for beam on). After a few seconds, the Therac-25 shut down. The console screen contained the message “Malfunction 54” and indicated a “treatment pause,” a low-priority problem. The dose monitor showed that the patient had received only 6 units of treatment rather than the desired 202 units. The operator hit the “P” (proceed) key to continue the treatment.

The cancer patient and the operator were in adjoining rooms. Normally, a video camera and intercom would enable the operator to monitor her patients. However, at the time of the accident neither system was operational.

The patient had received eight prior treatments, so he knew something was wrong as soon as the ninth treatment began. He was instantly aware of the overdose—he felt as if someone had poured hot coffee on his back or given him an electric shock. As he tried to get up from the table, the accelerator delivered its second dose, which hit him in the arm. The operator became aware of the problem when the patient began pounding on the door. He had received between 80 and 125 times the prescribed amount of radiation. He suffered acute pain and steadily lost bodily functions until he died from complications of the overdose five months later.

Second AECL Investigation, March 1986

After the accident, the ETCC shut down its Therac-25 and notified AECL. AECL sent out two engineers to examine the system. Try as they might, they could not reproduce Malfunction 54. They told the physicians it was impossible for the Therac-25 to overdose a patient, and they suggested

that the patient may have received an electrical shock due to a fault in the hospital's electrical system.

The ETCC checked out the electrical system and found no problems with it. After double-checking the linear accelerator's calibration, they put the Therac-25 back into service.

Tyler, Texas, April 1986

The second Tyler, Texas, accident was virtually a replay of the prior accident at ETCC. The same technician was in control of the Therac-25, and she went through the same process of entering X-ray when she meant electron beam, then going back and correcting her mistake. Once again, the machine halted with a Malfunction 54 shortly after she activated the electron beam. This time, however, the intercom was working, and she rushed to the treatment room when she heard the patient moan. There was nothing she could do to help him. The patient had received a massive dose of radiation to his brain, and he died three weeks later.

After the accident, ETCC immediately shut down the Therac-25 and contacted AECL again.

Yakima, Washington, January 1987

A second patient was severely burned by the Therac-25 at Yakima Valley Memorial Hospital under circumstances almost identical to those of the December 1985 accident. Four days after the treatment, the patient's skin revealed a series of parallel red stripes—the same pattern that had perplexed the radiation staff in the case of the previous patient. This time, the staff members were able to match the burns to the slots in the Therac-25's blocking tray. The patient died three months later.

Therac-25 Declared Defective, February 1987

On February 10, 1987, the FDA declared the Therac-25 to be defective. In order for the Therac-25 to gain back FDA approval, AECL had to demonstrate how it would make the system safe. Five months later, after five revisions, AECL produced a corrective action plan that met the approval of the FDA. This plan incorporated a variety of hardware interlocks to prevent the machine from delivering overdoses or activating the beam when the turntable was not in the correct position.

8.5.3 Software Errors

In the course of investigating the accidents, AECL discovered a variety of hardware and software problems with the Therac-25. Two of the software errors are examples of race conditions. In a **race condition**, two or more concurrent tasks share a variable, and the order in which they read or write the value of the variable can affect the behavior of the program. Race conditions are extremely difficult to identify and fix, because usually the two tasks do not interfere with each other and nothing goes wrong. Only in rare conditions will the tasks actually interfere with each other as they manipulate the variable, causing the error to occur. We describe both of these errors to give you some insight into how difficult they are to detect.

The accidents at the ETCC occurred because of a race condition associated with the command screen (Figure 8.4). One task was responsible for handling keyboard input and making changes to the command screen. A second task was responsible for monitoring the command screen for changes and moving the magnets into position. As shown in Figure 8.4, after the operator uses the first task to complete the prescription (1), the second task sees the cursor in the lower right-hand corner of the screen and begins the eight-second process of moving the magnets (2). Meanwhile, the operator sees her mistake. The first task responds to her keystrokes

and lets her change the “X” to an “E” (3). She gets the cursor back to the lower right-hand corner before eight seconds are up (4). Now the second task finishes moving the magnets (5). It sees the cursor in the lower right-hand corner of the screen and incorrectly assumes the screen has not changed. The crucial substitution of electron beam for X-ray goes unnoticed.

Figure 8.4

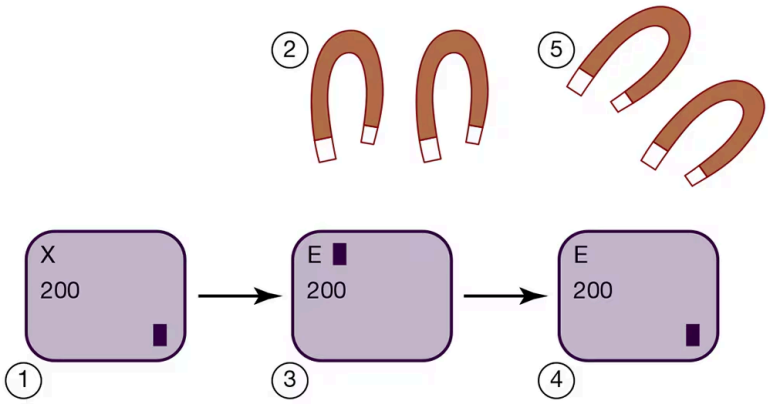


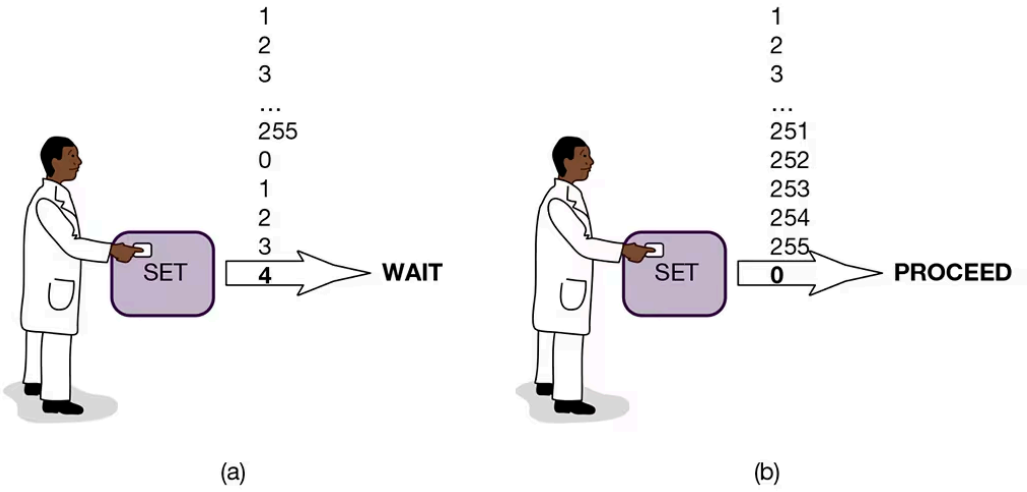
Illustration of a Therac-25 bug revealed by fast-typing operators. (1) The operator finishes filling in the form. The software knows the form is filled in because the cursor is in the lower right-hand corner of the screen. (2) The software instructs the magnets to move into the correct positions. While the magnets are moving, the software does not check for screen edits. (3) The operator changes the prescription from X-ray to electron beam. (4) The operator finishes the edit, returning the cursor to the lower right-hand corner of the screen. (5) The magnets finish moving. The software now checks the screen cursor. Since it is in the lower right-hand corner, the program assumes there have been no edits.

What makes this bug particularly treacherous is that it only occurs with faster, more experienced operators. Slower operators would not be able to complete the edit and get the

cursor back to the lower right-hand corner of the screen in only eight seconds. If the cursor happened to be anywhere else on the screen when the magnets stopped moving, the software would check for a screen edit and there would be no overdose. It is ironic that the safety of the system actually decreased as the experience of the operator increased.

Another race condition was responsible for the overdoses at the Yakima Valley Memorial Hospital (Figure 8.5). It occurred when the machine was putting the electron beam gun back into position. A variable was supposed to be 0 if the gun was ready to fire. Any other value meant the gun was not ready. As long as the electron beam gun was out of position, one task kept incrementing that variable. Unfortunately, the variable could only store the values from 0 to 255. Incrementing it when it had the value 255 would result in the variable's value rolling over to 0.

Figure 8.5



The Therac-25 could administer radiation too soon if the operator hit the SET button at precisely the wrong time. As long as the electron beam gun was out of position, a software task kept incrementing an 8-bit variable. (a) Usually when the operator hit the SET button, the variable was not zero and the system would wait, just as it was supposed to. (b) If the operator h the SET button just as the variable rolled over from 255 to 0, the system would administer radiation, even though the gun was out of position.

As illustrated in Figure 8.5, nearly every time that the operator hit the SET button when the gun was out of position, the variable was not 0 and the gun did not fire (a). However, there was a very slight chance that the variable would have just rolled over when the operator hit the SET button (b). In this case the accelerator would emit a charge, even though the system was not ready.

8.5.4 Postmortem

Let's consider some of the mistakes AECL made in the design, development, and support of this system.

When accidents were reported, AECL focused on identifying and fixing particular software bugs. This approach was too narrow. As Nancy Leveson and Clark Turner point out, "Most accidents are system accidents; that is, they stem from complex interactions between various components and activities" [51]. The entire system was broken, not just the software. A strategy of eliminating bugs assumes that at some

point the last bug will be eradicated. But as Leveson and Turner write, “There is always another software bug” [**51**].

The real problem was that the system was not designed to be fail-safe. Good engineering practice dictates that a system should be designed so that no single point of failure leads to a catastrophe. By relying completely upon software for protection against overdoses, the Therac-25 designers ignored this fundamental engineering principle.

Another flaw in the design of the Therac-25 was its lack of software or hardware devices to detect and report overdoses and shut down the accelerator immediately. Instead, the Therac-25 designers left it up to the patients to report when they had received overdoses.

There are also particular software lessons we can learn from the case of the Therac-25. First, it is very difficult to find software errors in programs where multiple tasks execute at the same time and interact through shared variables. Second, the software design needs to be as simple as possible, and design decisions must be documented to aid in the maintenance of the system. Third, the code must be reasonably documented at the time it is written. Fourth, reusing code does not always increase the quality of the final product. AECL assumed that by reusing code from the

Therac-6 and Therac-20, the software would be more reliable. After all, the code had been part of systems used by customers for years with no problems. This assumption turned out to be wrong. The earlier codes did contain errors, but these errors remained undetected because the earlier machines had hardware interlocks that prevented the computer's erroneous commands from harming patients.

The tragedy was compounded because AECL did not communicate fully with its customers. For example, AECL told the physicists in Washington and Texas that an overdose was impossible, even though AECL had already been sued by the patient in Georgia.

8.5.5 Moral Responsibility of the Therac-25 Team

Should the developers and managers at AECL be held morally responsible for the deaths resulting from the use of the Therac-25 they produced?

In order for a moral agent to be responsible for a harmful event, two conditions must hold:

- *Causal condition*: The actions (or inactions) of the agent must have caused the harm.
- *Mental condition*: The actions (or inactions) must have been intended or willed by the agent.

In this case, the causal condition is easy to establish. The deaths resulted both from the action of AECL employees (creating the therapy machine that administered the overdose) and the inaction of AECL employees (failing to withdraw the machine from service or even inform other users of the machine that there had been overdoses).

What about the second condition? Surely the engineers at AECL did not intend or try to create a machine that would administer lethal overdoses of radiation. However, philosophers also extend the mental condition to include unintended harm if the moral agent's actions were the result of carelessness, recklessness, or negligence. The design team took a number of actions that fall into this category. It constructed a system without hardware interlocks to prevent overdoses or to keep the beam from being activated when the turntable was not in a correct position. The machine had no software or hardware devices to detect an accidental overdose. Management allowed software to be developed

without adequate documentation. It presumed the correctness of reused code and failed to test it thoroughly. For these reasons the mental condition holds as well, and we conclude the Therac-25 team at AECL is morally responsible for the deaths caused by the Therac-25 radiation therapy machine.

8.5.6 Postscript

Three decades after the Therac-25 accidents, computer errors related to radiation machines continued to maim and kill patients. In late 2006, Scott Jerome-Parks received three overdoses from a linear accelerator at a New York City hospital that led to his death a few weeks later. He was only 43 years old. About the same time, at another New York hospital, 32-year-old patient with breast cancer Alexandra Jn-Charles received 27 straight days of radiation overdoses that led to her death. An investigation of radiation overdoses by the *New York Times* concluded that a variety of errors, including faulty software, were leading to crippling or fatal accidents [**52**].

8.6 Tesla Version 7.0 (Autopilot)

8.6.1 Introduction

In October 2014, Tesla began selling sedans with a $4,250 technology package containing a dozen ultrasonic sensors, a camera, a front radar, and digitally controlled brakes. The package allowed the car to stop before crashing. A year later, Tesla released a software update named Tesla Version 7.0 to the 60,000 cars it had sold with the technology package. The new software enabled the car to control its speed and steer. Tesla gave this update the nickname Autopilot and touted it as a safety improvement [53, 54].

With the launch of Tesla Version 7.0, Tesla Motors became the first automaker to release a product exhibiting characteristics of Level 3 automation, as defined by SAE International [55]:

- SAE Level 0—No Automation: “the full-time performance by the human driver of all aspects of the

dynamic driving task, even when enhanced by warning or intervention systems"

- SAE Level 1—Driver Assistance: "the driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task"
- SAE Level 2—Partial Automation: "the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task"
- SAE Level 3—Conditional Automation: "the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene"
- SAE Level 4—High Automation: "the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human

driver does not respond appropriately to a request to intervene”

- SAE Level 5—Full Automation: “the full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver”

8.6.2 May 2016 Fatal Accident

Joshua Brown was a 40-year-old Tesla fanatic. He nicknamed his Model S sedan Tessy, and he averaged more than 5,000 miles per month on the road [**56**]. Mr. Brown posted YouTube videos showing himself “driving” hands-free and testing the limits of the system [**57**, **58**, **59**]. He enjoyed driving fast and received eight speeding tickets over a six-year period, the most recent being a ticket in October 2015 for driving 64 miles per hour in a 35 mph zone [**60**].

At 4:36 p.m. on May 7, 2016, Brown was killed when his car crashed into the semitrailer portion of a semitrailer truck on a Florida highway. The accident occurred as Brown’s Model S, with Autopilot engaged, was traveling east on US-27A, a

divided highway in northern Florida. The semitrailer truck, traveling in the opposite direction on the highway, turned left in front of the Tesla. The semitrailer was high enough off the ground that the car continued under the semitrailer, shearing off its roof. The car coasted off the road and struck two wire fences and a power pole before coming to a stop [**61**].

The National Traffic Safety Board (NTSB) investigated the fatal accident. It retrieved from Brown's Tesla the standard SD nonvolatile memory card that recorded vehicle state and emergency event information, and it examined the data with the assistance of Tesla Motors. The NTSB analysis revealed that in the last six minutes before the crash, Brown had set the automobile's cruising speeds successively higher: first 47 mph, then 65 mph, 70 mph, and finally 74 mph. The automobile continued to travel at 74 mph, nine mph above the posted speed limit of 65 mph, for about two minutes until the collision with the semitrailer [**62**].

The NTSB investigation also determined that Autopilot was engaged for 37 minutes before the collision, and during this time Brown's hands were on the steering wheel for only 25 seconds. He received seven visual warnings to put his hands back on the steering wheel. On six of these occasions, the visual warning was followed by an audible chime. Brown

responded to each of these chimes by putting his hands on the steering wheel for between one and three seconds [**62**].

Neither Autopilot nor Brown applied the brakes before the crash [**62**]. According to the NTSB, Brown should have been able to see the semitrailer truck seven seconds before the crash because the accident occurred on a straight section of highway [**63**]. Why didn't the Automatic Emergency Braking (AEB) system of Tesla Version 7.0 activate when the semitrailer truck turned in front of the Tesla and Brown failed to respond? Mobileye, which supplied the vision system for Autopilot, provided one explanation. The system was designed to avoid rear-end collisions, not to avoid vehicles crossing laterally [**64**]. After Mobileye issued its statement, Tesla Motors quickly released a clarification in which it noted its autopilot system utilizes dozens of technologies to determine how it should respond to a particular situation. According to Tesla, automatic braking did not engage because the trailer was white, making it difficult to see, and the trailer was tall, making its radar signature similar to the radar signature of an overhead sign [**64**].

8.6.3 The Hand-off Problem

Several months before the fatal Tesla accident, Ken Washington, the vice president of research and advanced engineering at Ford Motor Company, said Ford was skipping over SAE Level 3 automation because of its inherent difficulties, namely: how can the computer ensure the driver is paying enough attention that it can pass over control in case of an emergency? Drivers who are not needed 99.9 percent of the time are likely to get bored. Audi reported test results indicating it takes an average of three to seven seconds, but sometimes as many as ten seconds, for a driver to regain attention and take control of a vehicle in an emergency. In many emergency situations, there may not be seven to ten seconds for the driver to retake control of the vehicle before an accident occurs. This is called the **hand-off problem** [**65**]. Volvo and Google have joined Ford in deciding to skip over SAE Level 3 automation and develop self-driving cars that never expect humans to take over in an emergency situation [**66**].

Passing over control from the computer to the human is more difficult when a driver is distracted. The Model S sedan Brown was driving did not have a mechanism to ensure the driver kept attention on the road while Autopilot was engaged. In fact, people observed Tesla sedans traveling down freeways under the control of Tesla Version 7.0

software while the person in the driver's seat was sleeping [67].

8.6.4 Assigning Moral Responsibility

The death of Joshua Brown was preventable. How, then, should moral responsibility for his death be allocated among the truck driver, the engineers and managers of Tesla Motors, and Brown himself?

Let's begin by considering the driver of the semitrailer truck. He turned his rig left, into the path of Brown's car, forcing the car to slow down and/or turn if it were to avoid an accident. The truck driver told the Florida Highway Patrol that he did not see the Tesla, but an eyewitness traveling behind the semitrailer truck saw the Tesla coming and told the Florida Highway Patrol that the truck driver should have seen the Tesla before he began turning in front of the car [68]. In general, the driver of a vehicle that turns left in front of another vehicle going straight is at fault, and in fact the truck driver involved in the accident was cited for a right-of-way violation [69]. However, Brown's car was exceeding the speed limit. When the vehicle going straight is speeding, some

or all of the fault typically shifts to the driver of the speeding car.

How much of the responsibility for the accident should be assigned to Joshua Brown? At the time of the accident Brown was flouting both traffic laws and Tesla Motors' instructions for the use of its product. He set the cruise control to 74 mph, nine mph above the speed limit, and he did not keep his hands on the steering wheel while Autopilot was engaged. The fact that he did not apply the brakes before the collision, even though the truck was in view for about seven seconds, is evidence he was not keeping his eyes on the road ahead.

Should the engineers and managers at Tesla Motors be held morally responsible for the accident that killed Joshua Brown? For them to be morally responsible, their actions or inactions must have caused the harm, and these actions must have been the result of carelessness, recklessness, or negligence. They did contribute to the harm by producing an automobile equipped with an Automatic Emergency Braking system that failed to stop the car before it collided with a large truck crossing in front of it. They demonstrated carelessness, recklessness, or negligence in three ways. First, they could have reduced the risk to drivers using the beta version of the Autopilot system by restricting its use to

freeways, where there is no lateral crossing traffic, but they chose not do so. Second, they decided to allow the driver to set an Autopilot cruising speed well over the speed limit, further stressing the capabilities of the computerized system. Third, and most significantly, they decided to release a product with SAE Level 3 automation capabilities without solving the hand-off problem. Tesla Version 7.0 did not even require drivers to demonstrate a minimal level of attention by keeping their hands on the steering wheel. Tesla engineers designed the Autopilot system so that it would continue to function even after issuing a series of warnings to the driver to put their hands back on the steering wheel. Tesla Motors implicitly acknowledged this problem by changing way the system worked after the fatal accident. In Tesla Version 8.0, Autopilot disengages if a driver ignores more than three warnings in one hour to put their hands back on the wheel [70].

Tesla Motors has marketed its automobiles by offering state-of-the-art technology to its customers, giving them "a tantalizing sneak preview of our self-driving future" [71]. In January 2016 Elon Musk said the Model S with Autopilot enabled was "probably better than humans at this point in highway driving" and predicted that Tesla cars would be capable of driving across the United States by 2018 [72].

Musk even retweeted news reports that showed drivers using Autopilot without their hands on the steering wheel [73]. Meanwhile, Tesla Motors has attempted to avoid legal liability for accidents caused by this new technology by expressing in writing that the "driver is still responsible for, and ultimately in control of, the car" [54]. The company is trying to have it both ways. The engineers and managers at Tesla Motors may not be held legally liable for the accident, but they do carry some moral responsibility.

In conclusion, moral responsibility for the accident that killed Joshua Brown must be shared (though not necessarily equally) among the truck driver, the engineers and managers at Tesla Motors, and Joshua Brown himself. The truck driver failed to yield the right of way to Joshua Brown's Tesla. Joshua Brown did not keep his hands on the steering wheel, set the cruising speed at 74 mph, and failed to remain attentive to the road ahead. Tesla Motors released to its customers an Automatic Emergency Braking system that failed to spot a large semitrailer truck crossing the path of Brown's Tesla. In addition, the decision was made to release a product with SAE Level 3 automation capabilities, despite the fact that the development team had not solved the hand-off problem.

8.7 Uber Test-Vehicle Accident

8.7.1 Introduction

Travis Kalanick, the co-founder and former CEO of ride-sharing company Uber, saw the development of autonomous vehicles as a threat to Uber's very existence. He felt if Uber were not among the first companies to develop the technology, then it would be put out of business by another ride-sharing enterprise that could undercut Uber's prices by eliminating the cost of drivers [74].

Uber moved quickly in an effort to catch up with other companies like Tesla and Waymo that had a big lead developing autonomous vehicles. In January 2015 it opened the Uber Advanced Technologies Center in Pittsburgh, Pennsylvania, and hired 50 autonomous-vehicle researchers from nearby Carnegie Mellon University [75]. Twenty months later, Uber started offering self-driving car pickups to customers in Pittsburgh. Note that the cars were self-driving, rather than fully autonomous: Uber engineers were still in the

front seat to monitor the system and take over when necessary [76].

On December 14, 2016, in defiance of California regulators, Uber publicly launched a similar service in San Francisco [77]. Uber's San Francisco experiment lasted only a week. A taxi driver caught on video a self-driving Uber running a red light in front of the Museum of Modern Art, generating a lot of negative media attention [78]. The California Department of Motor Vehicles revoked the registrations of Uber's self-driving cars, and Uber moved its test fleet to Arizona. Arizona governor Doug Ducey sent a Tweet welcoming Uber to his state: "While CA puts the brakes on innovation & change with more bureaucracy & regulation, AZ is paving the way for new technology & new businesses" [79].

8.7.2 Shift to One Human Safety Operator

When Uber began its testing of self-driving vehicles, it put two safety operators in the car: one behind the wheel and the other one in the front passenger seat. The first operator was responsible for taking over control of the vehicle from the computer system if necessary, and the second operator was

responsible for monitoring the performance of the system and logging significant events on a laptop computer.

Uber assigned its safety operators eight-hour shifts, with a 30-minute lunch break in the middle. Operators rode in self-driving cars that repeatedly traversed the same route. In the fall of 2017 Uber decided to remove the second safety operator. Some operators told their managers they were concerned that removing the second operator would make it more difficult for them to stay alert [80, 81].

The operators had a legitimate concern. Research going back for several decades has demonstrated that humans get bored when they are required to oversee highly automated systems that require relatively few interactions. Jobs that have been studied include train engineers [82], commercial airline pilots [83], drone operators [84], and surgical room anesthesiologists [85]. Uber itself fired one safety operator after the operator fell asleep at the wheel and was reported by another operator [80].

8.7.3 Effort to Eliminate "Bad Experiences"

The reliability of Uber's self-driving system in March 2018 was far lower than that of more mature systems. Whereas Waymo reported its cars traveled an average of 5,600 miles per intervention by a human safety operator, Uber's system was not yet consistently hitting the goal of averaging 13 miles per human intervention [80].

Another problematic issue for Uber was that every two miles on average its self-driving vehicles would startle passengers with a "bad experience," such as braking too quickly [81]. It is difficult to build a self-driving or autonomous car that can correctly avoid colliding with genuine obstacles, such as other cars and concrete medians, while ignoring other things detected by its sensors, such as car exhaust, steam, and litter. Incorrectly identifying a danger when in fact there is none is called a **false positive** (or, in common parlance, a false alarm). False positives are bad news. Not only is slamming on the brakes disconcerting to passengers, it is dangerous: a car that brakes more quickly than expected is liable to get rear-ended. In fact, getting rear-ended by a human driver is the most common type of accident for self-driving or autonomous cars [86]. Engineers can modify a system to eliminate nearly all false positives, but that action risks making the system prone to **false negatives:** failing to identify a dangerous situation, and that problem is even worse. A

great deal of testing is required to find the best middle ground.

New CEO Dara Khosrowshahi was supposed to visit Arizona in April 2018, and management wanted to give him a confidence-building “glitch-free ride” [80]. The decision was made to reduce the so-called “bad experiences” for passengers by turning off the emergency braking feature of the self-driving cars and giving responsibility for emergency braking and steering to the human safety operator. The engineers did not, however, implement a way for the self-driving system to alert the driver when emergency braking was needed. (The latter decision makes sense, actually. There was no point in implementing a driver alert when the system was generating a false positive every two miles. Drivers would soon learn to ignore the alarms.) [87].

The Volvo XC90s in Uber’s Arizona test fleet came equipped with an automatic emergency braking system as standard equipment, but that system was deactivated whenever the car was under the control of the self-driving computer system, to avoid a situation where two active systems would give conflicting commands to the vehicle [88].

)

8.7.4 March 18, 2018, Accident

At 9:14 p.m. on the evening of March 18, 2018, an Uber test vehicle left the Uber garage in Tempe, Arizona, and began running a predetermined test route with a vehicle operator in the driver's seat. At 9:58 p.m. the vehicle was in its second traversal of the test route when it crossed the Salt River, heading north in the rightmost lane of Mill Avenue at 43 miles per hour, two miles per hour below the speed limit. At this point the computer had been driving the car for 19 minutes without any intervention from the operator [89].

About 600 feet ahead of the Uber, a 49-year-old pedestrian wearing dark clothes stepped off the curb on the west side of Mill Avenue and began walking east across the street, pushing a bicycle. Mill Avenue was wide at the point they chose to cross, with two left turn lanes, two through lanes, and a bike lane. At the place the pedestrian began walking across the street, there was no crosswalk. Four signs in the vicinity warned pedestrians not to cross and directed them to use a crosswalk. The nearest crosswalk was located about 360 feet to the north [89].

About six seconds before impact the vehicle's sensors detected an object ahead. At first the self-driving system could not classify the object. It then classified the object as another vehicle before finally determining the object was a bicycle. For each of these classifications the system made predictions about the path the object would follow. When the car was about 80 feet from the pedestrian, 1.3 seconds before impact, the self-driving system determined that emergency braking would be required in order to prevent a collision. The self-driving system depended upon the human operator to perform the emergency braking. It did not alert the operator because there was no alert mechanism [**89**].

The safety operator had not been keeping their gaze fixed on the road ahead. Instead, they had been looking down frequently. They told the police they had been looking at the computer interface for several seconds and was surprised to see the pedestrian when they looked up [**88, 90**]. However, according to the police report, Hulu had streamed the talent show "The Voice" to the driver's smartphone that evening. The streaming lasted for 42 minutes and stopped at 9:59 p.m., "the approximate time of the collision" [**91**].

Less than a second before impact, the operator put their hands on the steering wheel and began turning the vehicle to

the right. Traveling at 39 miles per hour, the vehicle hit the pedestrian. Less than a second after the collision, the operator began braking the car. The pedestrian died as a result of being hit by the Volvo [89].

Videos from cameras inside the Uber reveal that the pedestrian did not look in the direction of the oncoming car until just before it hit them. If the pedestrian had looked for oncoming vehicles before stepping off the curb, the headlights of the Volvo might not have been visible to them because of a slight curve in the road and trees planted near the west side of the roadway. Perhaps they concluded there was no traffic at 10 p.m. and did not see a reason to look again. Perhaps their judgment was impaired. Toxicology tests performed by the medical examiner after the accident returned positive results for methamphetamine and marijuana [89].

A few days after the fatality, and just a few weeks after authorizing self-driving car developers to test vehicles with *no* human safety operators at the wheel, Governor Ducey put the brakes on Uber's testing program in Arizona. He said the safety of the public should have been Uber's top priority, and the March 18 incident was "an unquestionable failure to comply with this expectation" [92]. On May 23, 2018, Uber announced it was shutting down its test facility in Arizona

and terminated its 300 employees working there as safety operators [**93**].

8.8 Boeing 737 MAX

8.8.1 Background

The Boeing Company is one of the world's largest aerospace firms. Founded in 1916 in Seattle, Washington, the company's first contract was to build 50 seaplane trainers for the US Navy. Boeing played an important role in the Allied victory in World War II by producing the B-17 and B-29 bombers. In the 1950s, Boeing became a leader in commercial aviation. It produced the world's first commercially successful jetliner, the Boeing 707. The Boeing 727 was the first commercial jet to reach 1,000 sales, and the Boeing 737 was the first jet to surpass 10,000 sales [**94**].

At the beginning of the 21st century, however, Boeing found itself in a highly competitive situation with its principal rival: Airbus, a European consortium founded in 1970 [**95**]. In the important single-aisle market, Boeing's 737 had always prevailed over Airbus's A320, but in 2002 and every year thereafter Airbus surpassed Boeing in this category [**96**].

The Boeing 737 had taken its maiden flight in the spring of 1967 [**95**]. Over the next several decades, Boeing had

released new variants of the highly successful airplane. Still, the original design was nearly 40 years old. The premier product in the most important segment of the commercial jetliner market was now the Airbus A320 [**97**].

In 2005 Boeing began to develop plans for a new single-aisle jetliner [**98**]. Progress was slowed by a three-year delay in completing the new Boeing 787 Dreamliner [**97**]. Still, in January 2011, Boeing Chairman Jim McNerney stated Boeing was "leaning towards" developing an all-new replacement for the Boeing 737 that would be available by 2020 [**99**].

Later that year, Boeing executives changed course. Airbus had announced a new model of its A320 jetliner, the A320neo, featuring more fuel-efficient engines, and American Airlines, an important Boeing customer, informed Boeing that it was ordering hundreds of A320neos from Airbus and would stop purchasing Boeing planes unless Boeing could develop a more competitive aircraft [**100**]. Boeing's executives calculated that designing a new single-aisle aircraft would cost the company $10 billion, whereas redesigning the 737 to accommodate new, more fuel-efficient engines would cost only $3 billion [**101**]. Developing a next-generation 737 would have additional benefits beyond saving the company

$7 billion. A brand-new plane wouldn't be ready until 2020. During that time Airbus would continue to build on its sales lead. A next-generation 737 could be delivered to customers much sooner, in part because an updated 737 would get quicker approval from the US Federal Aviation Administration (FAA). Finally, Boeing could assure airlines that pilots familiar with the 737 would not need simulator training before flying the new model [**102**]. Pilot training is a significant expense for airlines, and saving airlines that cost can boost sales. Boeing decided to call its new, more fuel-efficient plane the 737 MAX, and it created an aggressive timeline to develop the aircraft [**100**].

Boeing's planned offering was welcomed by its customers. American Airlines pledged to purchase 100 Boeing 737 MAX jets [**103**]. Other airlines quickly followed suit, making the 737 MAX the fastest-selling airplane Boeing had ever marketed. When Indonesia's Lion Air agreed to purchase 230 737s, including 201 of the new 737 MAX, for a total of $22 billion, that became the largest single order in the history of The Boeing Company [**104**]. Boeing was so confident experienced 737 pilots would not need simulator training to fly the 737 MAX, it promised Southwest Airlines a rebate of about $1 million per plane if simulator training turned out to be required after all [**105**].

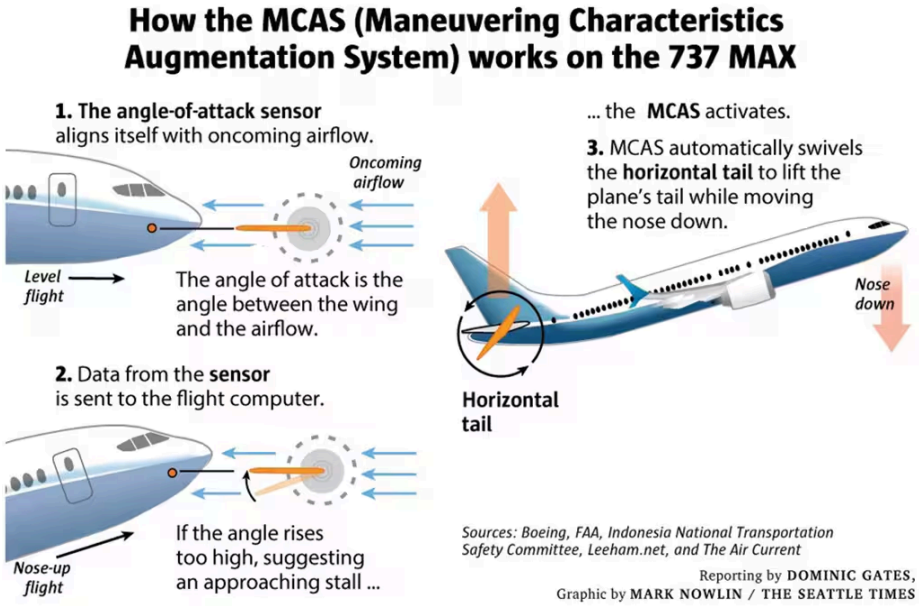
8.8.2 Engineering Challenges and Solutions

Putting more fuel-efficient engines on the 737 was easier said than done, however. The CFM International LEAP-1B engines were larger than those used on the previous model 737. To provide adequate ground clearance for the big new engines, Boeing engineers moved the engines forward and higher on the wings. Unfortunately, wind tunnel tests and simulator modeling revealed that the positioning of the new, larger engines increased lift and made the nose of the aircraft more likely to pitch up during a certain extreme banking maneuver called a "wind-up turn." When the nose pitched upward, the force the pilot felt on the control column suddenly disappeared, in violation of an FAA rule [**105**].

After trying and failing to solve the problem by making modifications to the wings, Boeing engineers turned to a software solution. They developed a new, computer-controlled Maneuvering Characteristics Augmentation System (MCAS). MCAS was designed to detect if the nose was pitching upward and to automatically swivel the horizontal stabilizer at the tail of the plane, pushing the aircraft's nose down (Figure 8.6). Since wind-up turns are

characterized by a high angle of attack (the angle between the oncoming air and the aircraft's centerline) and a high G force, the system activated when it received appropriate information from both an angle-of-attack sensor and a G-force sensor. The 737 MAX was equipped with two angle-of-attack sensors, one on each side of the fuselage. MCAS was designed to take input from only one of the sensors, alternating between them from one flight to the next [105].

Figure 8.6


How the MCAS (Maneuvering Characteristics Augmentation System) works on the 737 MAX
1. The angle-of-attack sensor aligns itself with oncoming airflow.
Oncoming airflow
Level flight
The angle of attack is the angle between the wing and the airflow.
2. Data from the sensor is sent to the flight computer.
Nose-up flight
If the angle rises too high, suggesting an approaching stall ...
... the MCAS activates.
3. MCAS automatically swivels the horizontal tail to lift the plane's tail while moving the nose down.
Nose down
Horizontal tail
Sources: Boeing, FAA, Indonesia National Transportation Safety Committee, Leeham.net, and The Air Current
Reporting by DOMINIC GATES,
Graphic by MARK NOWLIN / THE SEATTLE TIMES

The Boeing 737 MAX had a problem with the nose pitching up during certain maneuvers. Boeing designed the Maneuvering Characteristics Augmentation System to solve the problem.

(Mark Nowlin/The Seattle Times)

To make MCAS work, engineers had to disable a feature of previous models of the 737 and other Boeing planes that deactivated automatic functions to lower the nose when the

pilot pulled back hard on the control column. The control column still controlled the elevator tabs, but the nose-up force produced by the elevator tabs wasn't always enough to counteract the nose-down force produced by MCAS's swiveling of the horizontal stabilizer [**106**].

With these changes in place, the problem was solved. When the pilot executed a wind-up turn in flight simulator tests, MCAS automatically kept the nose from pitching up, and the control column forces changed smoothly throughout the maneuver.

8.8.3 Lack of Full Disclosure

Boeing engineers were now in a quandary. MCAS was the only way they had found to solve the issues related to the nose pitching upward, but introducing MCAS jeopardized the company's twin goals of achieving speedy FAA certification and avoiding the need for simulator training of existing 737 pilots. In July 2013 Boeing employees met and decided to describe MCAS to outsiders as an extension to Speed Trim, an existing system familiar to pilots and the FAA [**98**]. As a result, instead of taking a close look at MCAS, the FAA's certification process focused on what it saw as

potentially high-risk modifications, such as the larger engines and changes to the landing gear [**107**].

When Boeing began flight testing the 737 MAX in 2016, test pilots discovered that a similar "nose-up" issue arose in certain situations when the plane was flying at low speed. Engineers decided to use MCAS to solve this problem, too. However, for their solution to work, they had to make two significant changes to the system. First, to make MCAS effective at low speeds, they needed to increase the maximum stabilizer rotation from 0.6 degrees to 2.5 degrees each time MCAS was activated. Second, because slow-flying planes do not exhibit high G forces, they removed the necessity of a high reading from the G-force sensor for the MCAS system to activate. These changes made the MCAS system both more powerful and completely reliant on a single angle-of-attack sensor. Boeing did not disclose to the FAA these changes to MCAS [**102, 105, 108**].

It is an established engineering principle that safety-critical systems should not have a single point of failure. During the development of the 737 MAX, different engineers at Boeing expressed concerns about the MCAS relying upon a single angle-of-attack sensor. These concerns were dismissed. In the prevailing view, pilots would be able to follow well

established procedures for a runaway stabilizer to maintain control of the plane in the event of an AOA sensor failure. As a Boeing spokesperson told CNN, “Single sources of data are considered acceptable in such cases by our industry” [**109**].

Some inside Boeing were concerned by the fact that a Boeing test pilot had taken more than 10 seconds to respond to an unexpected activation of MCAS in a flight simulator. The test pilot had reported that the slow response to the problem had had “catastrophic” consequences [**98**]. Nevertheless, during flight testing of the aircraft, Boeing did not ask any of its test pilots to fly a scenario in which the AOA sensor failed and the MCAS activated [**105**]. Moreover, Boeing did not insist on providing its customers’ pilots with simulator training focusing on responding to an erroneous activation of MCAS. In fact, before taking delivery of the new plane, Lion Air asked Boeing: *Wouldn’t it be better if pilots had some simulation training before flying the 737 MAX?* Boeing replied to Lion Air, “There is absolutely no reason to require your pilots to require [sic] a MAX simulator to begin flying the MAX” [**102**].

Boeing did not include a description of MCAS in pilot manuals, even though pilots would be responsible for keeping the plane in the air if MCAS failed [**102, 105**]. Shortly after

the FAA approved the redesign of MCAS, Boeing's 737 chief technical pilot asked FAA's permission to remove references to MCAS from the flight crew operations manual. He justified the request by arguing that MCAS was "completely transparent to the flight crew and only operates WAY outside of the normal operating envelope" [98]. The FAA approved the request.

The cockpit of the 737 MAX contained an "AOA Disagree" warning light that was supposed to illuminate if one of the AOA sensors was not working properly. In 2017, after some planes had already been delivered, Boeing engineers discovered that due to a software error, the "AOA Disagree" warning light functioned only if a particular option package had been ordered. As a result, the warning light was inoperable on 80 percent of the aircraft that had been delivered, including those purchased by Lion Air and Ethiopian Airlines. Boeing did not share this information with the FAA or the airlines that had purchased the 737 MAX, and it continued delivering airplanes with the inoperable warning light [98, 106].

8.8.4 Lion Air Flight 610

On October 28, 2018, a Lion Air aircraft mechanic in Denpasar, Indonesia, working on a 737 MAX that had been delivered two months earlier, replaced the left angle-of-attack (AOA) sensor that had been giving faulty speed and altitude readings. The installation test did not reveal that the newly installed AOA sensor had a 21-degree bias [**110**].

When the plane was flown that day on a Lion Air flight from Denpasar to Jakarta, the bias in the AOA sensor resulted in a variety of in-flight warnings and the activation of MCAS. Fortunately, the flight crew was able to neutralize MCAS by flipping two switches labeled STAB TRIM to the CUTOUT position, which cut power to the horizontal stabilizer, as directed by the "runaway stabilizer" non-normal checklist (Figure 8.7). The pilot reported the malfunction, but he did not include in his log the use of the stabilizer trim cutout switches to solve the problem. Because the AOA Disagree warning light was inoperable on the plane, the flight crew did not have the opportunity to identify and log a malfunctioning AOA sensor as the source of the problem [**98**, **110**].

Figure 8.7

The following day, the same 737 MAX was used for Lion Air flight 610 from Jakarta. Two pilots, six flight attendants, and 181 passengers were on board. As soon as the nose gear left the runway, the faulty AOA sensor triggered a variety of cockpit warnings and alerts. A “stick shaker” on the captain’s control column began vibrating, erroneously warning him of an impending stall. The “Indicated Airspeed Disagree” warning message appeared, along with the “Altitude Disagree” message. About two minutes into the flight, MCAS activated, pushing the nose down. The captain and first officer engaged in a desperate tug-of-war with the flight control computer. They repeatedly pushed the nose up by activating the thumb-operated electric stabilizer trim switches, but neither pilot flipped the STAB TRIM switches to the CUTOUT position, and every time they let up on a stabilizer trim switch, MCAS re-engaged. MCAS activated at least 20 times, putting the plane into an unrecoverable nose-down position. The plane crashed into the Java Sea 11

minutes and 16 seconds after take-off, killing everyone on board [**110**].

8.8.5 Consequences of the Lion Air Crash

On November 6, 2018, Boeing released to airlines a flight crew operations manual bulletin for the 737 MAX. In the bulletin Boeing shared, “In the event of erroneous AOA data, the pitch trim system can trim the stabilizer nose down in increments lasting up to 10 seconds. The nose down stabilizer trim movement can be stopped and reversed with the use of the electric stabilizer trim switches but may restart 5 seconds after the electric stabilizer trim switches are released. Repetitive cycles of uncommanded nose down stabilizer continue to occur unless the stabilizer trim system is deactivated through use of both STAB TRIM CUTOUT switches.” The bulletin went on to advise pilots, “In the event an uncommanded nose down stabilizer trim is experienced, … [ensure] that the STAB TRIM CUTOUT switches are set to CUTOUT and stay in the CUTOUT position for the remainder of the flight.” [**111**]

The following day, the FAA issued an emergency airworthiness directive to all airlines operating the 737 MAX,

instructing them to revise their flight manuals to include the procedure outlined in the Boeing bulletin [**107**].

After Indonesia's National Transportation Safety Committee released a preliminary report on the Lion Air flight 310 crash, Boeing issued its own statement on November 27, 2018. The statement began by offering the company's condolences to the families of those aboard flight 310. It reassured its airline customers and their passengers that the 737 MAX was as safe as any other commercial airliner. The Boeing statement went on to raise suspicions about the quality of the maintenance procedures and pilots of Lion Air. It noted that the accident aircraft had experienced problems related to airspeed and altitude on each of the four flights occurring before Lion Air 610, despite various maintenance procedures being performed, including replacing the AOA sensor. It pointed out that on the flight preceding Lion Air 610, the crew followed the runaway stabilizer non-normal checklist and safely continued the flight. Finally, it questioned whether the pilots of Lion Air 610 had followed the procedures for a runaway stabilizer described in the flight crew operations manual [**112**].

After the Lion Air crash, the FAA began reviewing its certification process for MCAS. This was the first time the

FAA had been given a complete picture of how MCAS worked. Boeing proposed a redesign of MCAS, which the FAA accepted. In February 2019, Boeing and the FAA agreed that Boeing would complete its software update by April 12, 2019. The FAA completed a statistical analysis that concluded there would be another "15 accidents occurring over the life of the entire 737 MAX fleet if the software fix was not implemented" [**107**]. The FAA concluded that the risk of another crash was low enough that it could continue to allow 737 MAX aircraft to fly until the software fix was available in the summer of 2019 [**107**].

8.8.6 Ethiopian Airlines Flight 302

On March 10, 2019, Ethiopian Airlines Flight 302 took off from Addis Ababa, Ethiopia. The aircraft was a Boeing 737 MAX that had been delivered four months earlier. A total of 157 people were on board the plane. Soon after takeoff, the left AOA sensor began sending erroneous data to the flight control computer. The angle-of-attack reading was an impossible 74.5 degrees, yet the computer used this value to determine it should engage MCAS for 9 seconds [**106**].

The captain and first officer were bombarded with alerts. When the MCAS moved the stabilizer, the large stabilizer trim wheels on each side of the cockpit console spun rapidly. A variety of warning lights flashed on, indicating that the altitude and air speed readings on the instruments could not be trusted. The "stick shaker" loudly vibrated the captain's control column, warning him (incorrectly) that the plane was in danger of stalling. A loud clacker warned (correctly) that the jet was traveling too fast. A computerized voice repeatedly said, "Don't sink!"—warning that the plane's altitude was too low. The message "PULL UP" appeared on the flight displays [**105, 113**].

The captain pulled back on the control column and used the stabilizer trim switches to bring the nose up. Five seconds after the captain stopped trimming the stabilizer, MCAS re-engaged. The captain directed the first officer to move the STAB TRIM CUTOUT switches to the CUTOUT position. This action prevented MCAS from moving the horizontal stabilizer any further and also disabled the captain's electric stabilizer trim switches. The other way to trim the stabilizer was to hand-crank one of the stabilizer trim wheels on either side of the console. Unfortunately, the pilots had not reduced the power to the engines after takeoff, and the plane was traveling at a very high speed, putting such high forces on the

horizontal stabilizer that the stabilizer trim wheels could not be moved by hand [**106**]. When the captain realized he could not keep the nose up by pulling on the control column, he returned the STAB TRIM CUTOUT switches to the NORMAL position, going against the instructions in the flight crew operations manual. By doing so, the captain regained use of the electric stabilizer trim switch. However, five seconds after the captain released his thumb, MCAS re-engaged. The plane dived while the captain and first officer unsuccessfully tried to stop the descent by pulling on their control columns. About five minutes after takeoff, the plane crashed 39 miles southeast of the airport, killing everyone on board [**113**].

,

8.8.7 Consequences of the Ethiopian Airlines Crash

The day after the crash of Ethiopian Airlines flight 302, China grounded the 737 MAX. The European Union and many other countries quickly followed suit [**114**]. Meanwhile, the US Secretary of transportation, Elaine Chao, took a commercial flight on a Boeing 737 MAX to reassure the public [**102**].

At the crash site, Ethiopian investigators found the jackscrew controlling the tail, and it was in a full nose-down position, implicating MCAS as the cause of the crash. When this information was revealed, President Donald Trump issued an emergency order of prohibition, grounding all flights of the 737 MAX in the United States until further notice [**102**].

An FAA investigation identified six major issues contributing to the two crashes. It required Boeing to implement corrective actions addressing all the issues before it would recertify the 737 MAX. We list each issue identified by the FAA, followed by Boeing's corrective action [**115**]:

1. **Use of a single angle-of-attack sensor to activate the MCAS.**

   Boeing updated the MCAS software to use inputs from both AOA sensors, ensuring that a single failed or erroneous AOA sensor would not activate MCAS.

2. **Repetitive MCAS commands. As soon as the pilot released the electric trim switch, the MCAS reset, allowing the system to issue repeated nose-down commands.**

Boeing changed the software to ensure MCAS activates only once per high-AOA event.

3. **Additive effect of MCAS trim commands. Every MCAS command rotated the horizontal stabilizer a fixed amount, regardless of the position of the stabilizer. After multiple MCAS commands, the angle of the stabilizer was so great that the pilot could not counter it through control of the elevators.**

   Boeing put a ceiling on the maximum rotation of the horizontal stabilizer through MCAS commands. The ceiling was chosen so that the pilot could continue to control the airplane after the MCAS system was activated.

4. **Flight crews were not able to quickly recognize and respond to the erroneous horizontal stabilizer movement.**

   Boeing revised or added eight procedures to the Airplane Flight Manual and proposed additional simulator training for flight crews focusing on

recognizing and responding to erroneous horizontal stabilizer movements.

5. **The AOA disagree indicator was an optional feature of the aircraft.**

   Boeing changed the implementation of the AOA DISAGREE indicator to ensure it was part of the standard equipment present on all planes.

6. **The replacement AOA sensor installed on the Lion Air aircraft was mis-calibrated during a repair, and the mis-calibration was not detected.**

   Boeing revised the maintenance manual for the AOA, adding an independent check at the end of the repair to ensure the sensor is properly calibrated. Boeing also created a new procedure whereby technicians need to use a test fixture to position each AOA vane and verify the sensor is accurate before returning an airplane to service.

8.8.8 Financial Impact of Crashes

After the Ethiopian Airlines Flight 302 crash, airlines around the world grounded all 387 Boeing 737 MAX aircraft that had been in service. The plane remained grounded until December 2020, when the FAA once again approved the aircraft for flight. During this time Boeing could not deliver the plane, and it shut down the 737 MAX factory.

The Department of Justice filed a fraud conspiracy case against Boeing. Boeing paid $2.5 billion to settle the case. The settlement included a $244 million criminal penalty, $1.77 billion to purchasers of the 737 MAX, and a $500 million fund to compensate families of the victims [**116**].

Other costs associated with the 20-month-long grounding were $4 billion to shut down and start up the 737 MAX factory and $8 billion in compensation to airlines for lost revenues [**117**]. In all, the 737 MAX crashes cost Boeing about $20 billion [**118**].

8.8.9 Moral Responsibility of The Boeing Company

Should engineers and managers at The Boeing Company involved in the development of the 737 MAX be held morally

responsible for the deaths resulting from the Lion Air Flight 610 and Ethiopian Airlines Flight 302 crashes?

Recall that for a moral agent to be responsible for a harmful event, two conditions must hold:

- *Causal condition*: The actions or inactions of the agent must have caused the harm.
- *Mental condition*: The actions or inactions of the agent must have been intended or willed by the agent, or the agent must have been careless, reckless, or negligent.

The causal condition is easy to establish. Both crashes were directly linked to a serious malfunction of the Boeing 737 MAX aircraft.

Regarding the mental condition, there are a variety of ways in which the Boeing team was negligent. The crashes would probably not have occurred had the design of MCAS been changed in any of the following ways:

- Using inputs from both AOA sensors to determine if MCAS should be activated
- Allowing MCAS to activate only once per high-AOA event

- Putting a ceiling on the maximum rotation of the horizontal stabilizer through MCAS commands

Additionally, Boeing did not inform the FAA and its customers that the AOA Disagree light was not working on 80 percent of the planes it was delivering, including the planes involved in the two crashes. If the AOA Disagree light had been working on the Lion Air jet, the crew of the flight before Lion Air 610 would have had the opportunity to note the fact in its log, which may have allowed the problem to be fixed before Lion Air 610 took off.

Furthermore, Boeing was relying on pilots to quickly execute the runaway stabilizer procedure in case a faulty AOA sensor triggered the MCAS. Boeing knew that taking more than 10 seconds to respond to the MCAS activation could result in a catastrophe, but it assumed pilots would be able to respond more rapidly than that, not adequately considering the distraction caused by the cacophony of alerts associated with AOA sensor failure and MCAS activation. Boeing did not have its own pilots flight test a scenario in which the AOA sensor failed and the MCAS activated. Not only did Boeing not require that pilots migrating to the 737 MAX undergo simulator training focusing on recognizing and responding to a runaway stabilizer, it insisted to its airline customers that

there was “absolutely no reason” for any simulator training before 737 pilots began flying the 737 MAX. Finally, it removed any mention of MCAS from the flight crew operations manual.

Those whose actions or inactions contributed to the following design, implementation, and policy decisions share moral responsibility for the deaths resulting from the Lion Air Flight 610 and Ethiopian Airlines Flight 302 crashes:

- Relying on a single AOA sensor to activate MCAS
- Allowing MCAS to activate multiple times per high-AOA event
- Not putting a ceiling on the horizontal stabilizer rotation through MCAS commands
- Not informing the FAA and airlines that the AOA Disagree light was not working
- Not flight testing an AOA sensor failure scenario
- Not informing airline pilots of MCAS
- Not providing simulator training to airline pilots focusing on recognizing and responding to a runaway horizontal stabilizer

8.9 Algorithmic Bias

A variety of factors can contribute to people making poor decisions. These factors may include mis-prioritizing emotions and logic, putting too much weight on the opinions of others, and only considering information that confirms existing biases [**119**]. Automated decision-making systems have been deployed with the intention of replacing slow, subjective, prejudiced humans with fast, objective, data-driven computers. Reducing labor costs is another motivation for switching to an automated decision-making system [**120**]. Unfortunately, history has shown that computerized systems can make poor decisions too.

8.9.1 Bias in Computer Systems

Rapid growth in the deployment of AI-based decision-making systems has raised the urgency of policy discussions about the impact of these systems on historically marginalized groups. According to Batya Friedman and Helen Nissenbaum, a computer system is **biased** if it "systematically and unfairly … denies an opportunity or a good or if it assigns an

undesirable outcome to an individual or group of individuals on grounds that are unreasonable or inappropriate" [**121**]. **Algorithmic bias** refers to bias demonstrated by a decision-making AI system based on machine learning. Friedman and Nissenbaum identified three types of bias: preexisting bias, technical bias, and emergent bias [**121**].

A computer system demonstrates **preexisting bias** if it incorporates biases existing "in social institutions, practices, and attitudes" before the system's development [**121**]. An AI decision-making system can demonstrate preexisting bias if it is trained on a data set that either is not representative of the population or incorporates historical social injustices. For example, a data set widely used to train facial-recognition systems was not representative of the general population: about 75 percent of the faces were of men, and more than 80 percent of the faces were of white people. A researcher at MIT's Media Lab found that the facial recognition systems of Microsoft, IBM, and Face++ demonstrated preexisting bias. They misidentified the gender of fair-skinned men only 1 percent of the time, while they misidentified the gender of darker-skinned women up to 35 percent of the time [**122**].

Technical bias refers to bias that results from how designers resolve issues related to the technical limitations of a

computer system. For example, Google search results are presented in a particular order, and only so many results can fit on the first page. The #1 result has a click-through rate of 27.6 percent, more than 10 times the click through rate of the #10 result; less than 1 percent of Google searchers click on a result from the second page [**123**]. Therefore, the algorithm that chooses the order in which search results are presented could introduce bias into the system.

Emergent bias is bias that arises as a computer system is used. The deployment of Tay is a prime example of emergent bias. On March 23, 2016, Microsoft launched via Twitter a chatbot called Tay. Tay was designed to talk "like a teen girl" and entertain 18- to 24 year olds in the United States. Tay modified its communications based on user input, and some malicious users quickly began feeding it misinformation and politically incorrect phrases. Before the day was out, Tay was "tweeting some of the most offensive racial slurs, spreading hate speech, [and] promoting Nazism" [**124**]. Microsoft took Tay offline within 24 hours of its release, and it apologized for the "unintended offensive and hurtful tweets" [**125**].

8.9.2 Image Recognition Systems

Google Photos, released in 2015, employs machine learning to group photos automatically based on their contents, allowing users to search their image collections. Soon after the service began, Jacky Alcine, a 21-year-old Black computer programmer, tweeted that Google Photos had mislabeled him and a Black friend as “gorillas” in photos he had posted. Google quickly responded to the tweet by issuing an apology and censoring the words “gorilla,” “chimp,” “chimpanzee,” and “monkey” from Google Photos searches and image tags until the problem could be fixed. Eight years later, Google Photos still did not support visual searches for primates [126].

In two important collections of photos used by machine-learning algorithms, most images of cooking, washing, and shopping show women, and most images of coaching and shooting show men. When you think about where images come from, it's not surprising that the images tend to show people in stereotypical roles. However, you might be surprised to learn that machine-learning systems can amplify preexisting biases. One study showed that while a training set

of photos had women in 67 percent of the photos illustrating cooking, the trained system identified the person in 84 percent of the cooking photos as a woman [**127**, **128**].

8.9.3 Speech Recognition Systems

Automated speech recognition capabilities are embedded in a wide variety of devices, including smartphones, home appliances, and automobiles. Automated speech recognition has also allowed companies to improve the accessibility of their products. For example:

- automated subtitling makes video content more accessible to people with hearing loss;
- people with loss of vision can use speech recognition software to create documents; and
- hands-free computing makes computers more accessible to people with a loss of motor skills.

A group of researchers from Stanford University and Georgetown University tested automated speech recognition systems developed by Amazon, Apple, Google, IBM, and Microsoft. Their analysis was based on 20 hours of audio

recordings from two sources. The first source was the Corpus of Regional African American Language, and the second was Voices of California. All told, the research team analyzed the performance of the speech recognition software on 42 white speakers and 72 Black speakers from five US cities. They discovered all five of these systems did a better job understanding white speakers than Black speakers. Overall, the average word error rate was 17 percent for white women, 21 percent for white men, 30 percent for Black women, and 41 percent for Black men. The researchers concluded that to reduce the error rate, machine learning systems need to be trained on more diverse datasets that include African American Vernacular English [**129**].

8.9.4 Impact Pro

To reduce healthcare costs, health systems use algorithms to identify high-risk patients who should be enrolled in special care management programs. These programs provide patients with greater access to doctors and nurses who can help prevent the worst outcomes, improve patient satisfaction, and keep costs under control.

A group of researchers had access to the medical records of about 50,000 patients at a large academic hospital, including

the patients' risk scores generated by Impact Pro, a product of UnitedHealth Group [**130**]. Patients who scored above the 97th percentile were automatically identified as eligible to enroll in a special care management program. Patients who scored above the 55th percentile were referred to their primary care physician, who then made a recommendation about whether they would benefit from the program. The researchers discovered that the tool gave less-healthy Black people the same scores as more-healthy white people. As a result, Black people were disproportionately excluded from the special care management program.

The scoring algorithm did not consider the race of the patients. How, then, did it end up scoring Black patients lower than white patients? The reason is that the algorithm assumed that patients with the highest current healthcare costs were at greatest risk for large healthcare costs in the future. To reduce future healthcare costs, it targeted patients with the highest current costs for the special care management program. However, Black patients generate lower healthcare costs than white patients with the same medical issues. Put another way, on average white patients get more treatment for their medical conditions than Black patients. In the data set used to train the AI system, health care costs turned out to be a **proxy**, or highly correlated

substitute, for the race of the patient. The authors conclude, "As a result, accurate prediction of costs necessarily means being racially biased on health" [**131**].

8.9.5 Credit Scoring

Access to credit is an important factor helping people get ahead financially. Home equity is the largest component of a typical US household's wealth [**132**], and nearly everyone needs a mortgage loan to purchase a home. During the Depression of the 1930s, the US government began insuring the mortgages of homeowners. Government officials created color-coded maps of 200 US cities showing the riskiness of the home loans by neighborhood. Red indicated those neighborhoods to be excluded from the program because the risk of property values declining was judged to be the highest. Most Black people lived in those neighborhoods and were excluded from getting home loans backed by government insurance [**133**]. This exclusion, called **redlining**, helps explain why to this day the home ownership rate of Black families in the United States is 46 percent, compared with a 76 percent home ownership rate among white US families [**134**]. The lack of home equity wealth is an important reason

why the wealth of the median Black household is only 10 percent the wealth of the median white household [**135**].

The Fair Housing Act of 1968 and the Equal Credit Opportunity Act of 1974 prohibited racial discrimination when offering credit. Modern credit scoring systems do not take race into account when computing credit scores. Nevertheless, it can be difficult to level the playing field completely. A recent study of credit data of 50 million people found that the accuracy of credit scores in predicting loan defaults was 5 percent lower for minority borrowers than for non-minority borrowers, and the accuracy of the predictions for low-income applicants was 10 percent worse than for higher-income applicants [**136**].

The reason for the disparity in accuracy is that minority and low-income applicants tend to have "thinner" credit histories, which can lower their credit scores in two ways. First, credit scores are lower for people who do not have a history of repaying loans. Second, "dings" in a credit file, such as a late payment on a credit card, have a larger impact on the credit score when the total amount of credit-related information is smaller [**137**].

Unfortunately, the preexisting bias of the credit scoring system is difficult to eliminate. Less accurate credit scoring

for the groups that have traditionally had a more difficult time obtaining credit can result in credit hysteresis, keeping people with "thinner" credit histories in that situation. Some experts have concluded that the solution lies not in designing a more sophisticated credit scoring algorithm. After all, the problem is that for many credit applicants there is not enough data to analyze. Instead, the solution lies in creating new opportunities for applicants with thin credit histories to provide data demonstrating their suitability to borrow money [137].

8.9.6 Predictive Policing

Predictive policing is the "collection and analysis of data about previous crimes" to identify people or areas where criminal activities are more likely to occur [138]. Police departments use predictive policing "to deploy their resources more efficiently and effectively" [138].

Predictive policing is a controversial topic. Proponents of predictive policing point out numerous successes. Here are three examples:

- Memphis, Tennessee, launched its Blue CRUSH (Crime Reduction Using Statistical History) program in 2007.

Six years later, serious crimes had fallen 30 percent and violent crimes were down 20 percent [**139**].

- The Santa Cruz, California, police department used predictive policing to focus on motor vehicle thefts as well as vehicular, residential, and commercial burglaries. Police officers beginning their shift would receive a map identifying 15 hot spots. Officers were asked to drive through these areas when they were not busy handling other calls. The department saw a 19 percent decline in burglaries over a six-month period [**140**].
- The Los Angeles, California, police department tested predictive policing in its Foothill Division, an area with 300,000 residents. During the test period, property crime in the Foothill Division declined 12 percent, compared with an increase of 0.4 percent in the rest of the city. Based on this result, the LAPD expanded to more divisions, and all of them experienced a drop in crime [**140**].

However, a literature review conducted by Albert Meijer and Martijn Wessels concluded that there was a lack of empirical evidence supporting claims that predictive policing is effective. Instead, support for predictive policing was based

more on “convincing arguments and anecdotal evidence” rather than empirical results [**138**].

Many groups, including the ACLU and the NAACP, have harshly criticized predictive policing systems as demonstrating preexisting biases against people of color. One of criticisms of the human rights groups is that minority neighborhoods have traditionally been over-policed. As a result, police records are not representative of the general population; they over-represent people of color and their neighborhoods [**141**]. Given that preexisting bias, the computer-driven system will direct a greater police presence in minority communities, leading to more arrests, and perpetuating the preexisting bias.

Another criticism of predictive policing is that it puts an unfair burden on innocent people. An innocent person who lives in a more heavily policed area is more likely to be stopped, questioned, searched, or arrested than an innocent person living in another part of town [**141**]. In this respect, predictive policing is like racial profiling.

A counterargument to the second criticism is that people of color may carry most of the burdens of predictive policing, but they also reap most of the benefits. Victims of crime in the United States are disproportionately Black people. Black

people constitute about 13 percent of the US population but comprise about 52 percent of murder victims. About 70 percent of Black crime victims identify a Black person as the perpetrator of the crime. Any disproportionate allocation of police resources to a Black neighborhood would disproportionately benefit Black victims [**141**].

Duncan Purves admits that the counterargument has merit, but he holds that members of the targeted neighborhoods have some moral authority to object to increased police patrols. Community members may conclude that the upside of a heightened police presence (fewer crimes) is not worth the downside (more traffic tickets, more drug arrests, more victims of police violence, etc.) [**141**]. Purves suggests three steps police departments can take to gain community support for its initiatives:

- pledging to use predictive policing to target serious crimes rather than minor offenses;
- community policing—engaging with community members to develop priorities and strategies; and
- problem oriented policing—working to eliminate the underlying causes of crimes [**141**].

Perhaps influenced by the criticism of predictive policing, Los Angeles stopped using the PredPol program in April 2020 [**142**]. Two months later, Santa Cruz became the first US city to ban predictive policing [**143**]. The Memphis Police Department continues to use Blue CRUSH [**144**].

8.9.7 COMPAS

Advocates of bringing data-supported decision making to the justice system argue that it can improve public safety by reducing "pretrial misconduct, post-conviction reoffending, and other forms of community harm resulting from crime" [**145**]. Some US states have developed defendant risk assessment tools, while others use a commercially developed tool. One of these commercial tools is COMPAS, which stands for Correctional Offender Management Profiling for Alternative Sanctions. COMPAS, developed by Northpointe (now Equivant), supports decision making in the legal system by assessing the recidivism risk of criminal defendants. In many courts across the United States, COMPAS scores inform judges' pretrial release and sentencing decisions.

COMPAS defines recidivism as "a finger-printable arrest involving a charge and a filing for any uniform crime reporting (UCR) code." Recidivism risk scores assigned to

defendants range from 1 to 10, where scores of 1 to 4 represent low risk, scores of 5 to 7 represent medium risk, and scores of 8 to 10 represent high risk.

Researchers from ProPublica studied more than 10,000 criminal defendants in Broward County, Florida, where COMPAS was being used to determine whether a defendant should be released or detained before their trial. Looking at defendants who did not recidivate within two years, they concluded that the COMPAS tool was biased against Black defendants [**146**]. Northpointe, the company producing COMPAS, offered a rebuttal to the ProPublica study, denying that the tool was biased [**147**].

The issue raised by the ProPublica study stimulated an important finding. It seems reasonable that a fair, unbiased recidivism-prediction tool would exhibit the following three properties:

1. The score assigned to a defendant should be an accurate indicator of the probability of recidivism, regardless of the defendant's race.

2. The average score assigned to defendants of one race who recidivate should be the same as the average score assigned to defendants of another race who recidivate.

3. The average score assigned to defendants of one race who do not recidivate should be the same as the average score assigned to defendants of another race who do not recidivate.

Unfortunately, it is mathematically impossible to achieve all three of these goals simultaneously unless the recidivism rates of the racial groups are identical, or the tool makes infallible predictions [148]. For all practical purposes, any tool will fail to exhibit at least one of the three properties mentioned above. ProPublica argued the COMPAS tool was unfair because it did not satisfy properties 2 and 3. Northpointe replied that its COMPAS tool was fair because it exhibited property 1. Unfortunately, there is no way the tool can satisfy all three fairness properties.

8.9.8 Definitions of Fairness

The deployment of biased computer systems using AI has prompted many critiques, and some software companies have publicly acknowledged the importance of developing unbiased systems from now on. To give just two examples, one of Microsoft's six principles of responsible AI is "AI systems should treat all people fairly," and Google has

articulated seven principles for responsible AI, including "Avoid creating or reinforcing unfair bias" [**149**, **150**]. However, creating an unbiased computer system is easier said than done.

To prevent a computer system from discriminating against a member of a protected class, you might think the best way to achieve that goal is to withhold information about protected class membership from the system. This is called "fairness by unawareness." Unfortunately, other pieces of data can become proxies for the sensitive data. Earlier, we saw how health care costs turned out to be a proxy for race in the Impact Pro system. Here's another example. Cities like Chicago and Detroit are highly segregated [**151**]. In these cities a person's nine-digit ZIP code is a reasonably reliable proxy for their race. It can be difficult, if not impossible, to remove from the data set not just sensitive data, such as race, but all the proxies for the sensitive data. Some suggest that rather than try to do that, it makes more sense for a computer system to collect information about individuals' protected characteristics so that post-decision analyses can be performed to determine whether the system treated members of protected classes fairly [**152**].

Still, we haven't answered the question: What does it mean to treat everyone fairly? There are many definitions of fairness. Unfortunately, not all of them can be satisfied simultaneously.

Let's compare three definitions of fairness: demographic parity, equality of opportunity, and equalized odds. To ground our discussion, we use the following imaginary example, inspired by entries in Google's Machine Learning Glossary [**153**].

For many years Ivy League University Law School has offered a summer short course on advanced legal topics. The program attracts most of its applications from people who live on the East Coast, but there are some applications from the West Coast too. (Apparently nobody living in the rest of the country is interested.) How do we know if the law school's process for accepting applicants into the program is fair?

Demographic parity (also called group fairness) is achieved if acceptance rates for the two groups are identical. For example, consider this outcome from one year's application pool:

	East Coast Applicants	West Coast Applicants

Applied	100	40
Accepted	41	10
Rejected	59	30

The acceptance rate for the applicants from the East Coast was 41 percent, while the acceptance rate for the applicants from the West Coast was 25 percent. Using demographic parity as our definition of fairness, the admissions process was not fair because the acceptance rates of the two groups were different.

An objection to the definition of fairness embodied in demographic parity is that it ignores any possible correlation between group membership and qualifications for the short course. Perhaps on average the West Coast applicants were less qualified for the short course than the East Coast applicants. **Equality of opportunity** is a different notion of fairness, holding that all people qualified for an opportunity should be equally likely to get that opportunity, regardless of which group they belong to.

Let's expand the previous table by dividing each group's applicants into two subsets: those qualified to take the short

course and those not qualified to take it.

	East Coast Applicants		West Coast Applicants	
	Qualified	Not Qualified	Qualified	Not Qualified
Applied	70	30	20	20
Accepted	35	6	10	0
Rejected	35	24	10	20

It turns out that 70 percent of the East Coast applicants were qualified, versus only 50 percent of the West Coast applicants. The admissions process satisfied equality of opportunity because it accepted 50 percent of the qualified applicants from both groups.

Two objections arise about the concept of fairness embodied in equality of opportunity. First, how can we be sure the decisions categorizing applicants as “Qualified” or “Not Qualified” were unbiased? Second, even if the applicants were correctly classified as qualified or not qualified, you could argue that the admissions process was still unfair to the West Coast applicants because 20 percent of the unqualified applicants from the East Coast were accepted, compared to

none of the unqualified applicants from the West Coast. The second objection leads us to our next definition of fairness.

Equalized odds is a principle of fairness holding that, regardless of which group they are in, all people qualified for an opportunity should be equally likely to get that opportunity, and all people unqualified for an opportunity should be equally likely to be rejected.

For example, suppose for the next summer workshop, Ivy League University Law School amends its acceptance process, resulting in the following outcome.

	East Coast Applicants		West Coast Applicants	
	Qualified	Not Qualified	Qualified	Not Qualified
Applied	70	30	20	20
Accepted	35	3	10	2
Rejected	35	27	10	18

The admissions program now satisfies the fairness criteria of equalized odds because it accepts 50 percent of the qualified applicants from both groups and rejects 90 percent of the unqualified applicants from both groups.

Note that if a process meets the equalized odds definition of fairness, it is also fair according to equality of opportunity, which is a looser definition of fairness. However, unless the percentage of qualified applicants is identical for both groups, a process that is fair according to equalized odds will not be fair according to demographic parity. In general, all three definitions of fairness cannot be satisfied simultaneously. Earlier, we saw the same outcome with a different set of fairness definitions used to evaluate the COMPAS system. Identifying context-appropriate definitions of fairness and choosing which definition of fairness to satisfy are important steps that should be taken by systems designers in consultation with the user community.

Summary

Computers are part of larger systems, and ultimately it is the reliability of the entire system that is important. A well-engineered system can tolerate the malfunction of any single component without failing. This chapter has presented many examples of how the computer or the computer-human interface turned out to be the "weak link" in the system, leading to a failure. These examples provide important lessons for computer scientists and others involved in the design, implementation, and testing of large systems.

Two sources of failure are data-entry errors and data-retrieval errors. While it's easy to focus on a particular mistake made by the person entering or retrieving the data, the system is larger than the individual person. For example, in the case of the 2000 general election in Florida, incorrect records in the computer database disqualified thousands of voters. The data-entry errors caused the *voting system* to work incorrectly. Sheila Jackson Stossier was arrested by police who confused her with Shirley Jackson. The data-

retrieval error caused the *criminal justice system* to perform incorrectly.

When the topics are software and billing errors, it is easier to identify the system that is failing. For example, when Qwest sent out 14,000 incorrect bills to its cellular phone customers, it's clear that the billing system had failed.

In **Sections 8.4** and **8.5**, we dissected several systems to determine the causes of their failures. The program for the Patriot missile's radar tracking system had a subtle flaw: a tiny truncation error occurred every time the clock signal was stored in a floating-point variable. Over a period of 100 hours, all those tiny errors added up to a significant amount, causing the radar system to lose its target. The Ariane 5 blew up because a single assignment statement caused the onboard computers to crash. The AT&T long-distance network collapsed because of one faulty line of code.

A well-engineered system does not fail when a single component fails. In the case of hardware, this principle is easier to apply. For example, a typical jetliner has two engines. It is designed to be able to fly on a single engine, so if one engine fails, the plane can still fly to the nearest airport and land. When it comes to software, the goal is much harder to meet. If we have two computers in the system, that

provides redundancy in case one of the computers has a hardware failure. However, if both computers are running the same software, there is no software redundancy. A software bug that causes one computer to fail will cause both computers to fail. The partial collapse of the AT&T long-distance network is an example of this phenomenon. All 80 switches containing the latest version of the software failed. Fortunately, 34 switches were running an older version of the software, which prevented a total collapse of AT&T's system.

Imagine what it would take to provide true redundancy in the case of software systems. Should companies maintain two entirely different billing systems so that the bills produced by one system could be double-checked by the other? Should the federal government support two completely different implementations of the National Crime Information Center? These alternatives seem unrealistic. On the other hand, redundancy seems much more feasible when we look at data-entry and data-retrieval operations. Two different data-entry operators could input records into databases, and the computer could check to make sure the records agreed. This would reduce the chance of bad data being entered into databases in the first place. Two different people could look at the results returned from a computer query, using their

own common sense and understanding to see if the output made sense. A paper audit trail is a practical way to add redundancy to an electronic voting machine.

While it may be infeasible to provide redundant software systems, safety-critical systems should never rely completely upon a single piece of software. The Therac-25 overdoses occurred because the system lacked the hardware interlocks of the earlier models.

The stories of computer system failures contain other valuable lessons. The Ariane 5 and Therac-25 failures show that it can be dangerous to reuse code. Assumptions that were valid when the code was originally written may no longer be true when the code is reused. Since some of these assumptions may not be documented, the new design team may not have the opportunity to check if these assumptions still hold true in the new system.

The automated baggage system at the Denver International Airport demonstrates the difficulty of debugging a complex system. Tackling one problem at a time, solving it, and moving on to the next problem proved to be a poor approach, because the overall system design had serious flaws. For example, BAE did not even realize that simply getting luggage carts to where they were needed in a fair and

efficient manner was an incredibly difficult problem. Even if BAE had solved all the low-level technical problems, this high-level problem would have prevented the system from meeting its performance goals during the busiest times.

Systems can fail because of miscommunications among people. The Mars Climate Orbiter is an example of this kind of failure. The software written by the team in Colorado used English units, while the software written by the team in California used metric units. The output of one program was incompatible with the input to the other program, but a poorly specified interface allowed this error to remain undetected until after the spacecraft was destroyed.

A self-driving automobile is a system, too. A computer may be responsible for driving the vehicle 99 percent of the time, but the human driver is supposed to take over when the situation is more than the computer can handle. Unfortunately, the Tesla Autopilot accident and the Uber test-vehicle accident demonstrate that humans do not perform well when they have nothing to do for long periods of time and then are required to snap to attention and immediately take over during an emergency.

The Boeing 737 MAX accidents provide another example of a system failing when the human response cannot quickly

correct a computer failure. To address flight control issues caused by larger engines, Boeing created the Maneuvering Characteristics Augmentation System and gave it an unprecedented amount of control over the horizontal stabilizer on the 737 MAX. Boeing assumed that pilots already trained to handle a runaway horizontal stabilizer would be able to respond immediately to an erroneous activation of the MCAS without any additional instruction or even knowledge of the system's existence. That mistaken assumption led to two crashes, 346 deaths, and a 21-month-long grounding of the 737 MAX.

AI- driven systems have been deployed in numerous domains where consequential decisions must be made. They have recommended who gets prioritized for preventative health care, who should be eligible for a loan, and whose neighborhood should be the target of extra police patrols. Unfortunately, computerized systems operating in all these domains have been found to be biased. It turns out that creating an unbiased computerized system is much easier said than done. For one thing, the choice of the data set used to train the system is critically important. Two examples of bad training data sets are sets that are not representative of the population and sets that incorporate historical social injustices. Another reason it is difficult to create an unbiased

computerized system is that in any domain, there are likely to be several mutually incompatible definitions of what is "fair." A system that is fair according to one reasonable metric may be unfair according to another reasonable metric.

Further Reading, Listening, and Viewing

- Mark Bailey and Keven McAlester. *Downfall: The Case Against Boeing*. Netflix, February 18, 2022. 89 minutes.

- Greg Bensinger. "Why Tesla's 'Beta Testing' Puts the Public at Risk." *New York Times*, July 30, 2021. https://www.nytimes.com/2021/07/30/opinion/self-driving-cars-tesla-elon-musk.html.

- Walt Bogdanich. "Radiation Offers New Cures, and Ways to Do Harm." *New York Times*, January 23, 2010.

- Walt Bogdanich. "As Technology Surges, Radiation Safeguards Lag." *New York Times*, January 26, 2010. www.nytimes.com.

- Joy Buolamwini. "How I'm Fighting Bias in Algorithms." *TEDxBeaconStreet*, viewed June 16, 2018. 8:45. www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms.

- Sean Clark. "Cruisin' in a New Cadillac. . . No Hands!" *CNN Money* (Web site), money.cnn.com/video/news/2017/10/11/cadillac-super-cruise-washington-dc.cnnmoney/index.html. Accessed May 5, 2018.

- Mary Cummings. Interview by Nicole Laskowski. *SearchCIO*. "Automated Systems Problems and Dangers: Employee Boredom." June 26, 2015. 2:14. searchcio.techtarget.com/video/One-danger-of-automated-systems- Employees-get-bored.

- Alex Davies. "The Very Human Problem Blocking the Path to Self-Driving Cars." *Wired,* January 1, 2017.

- Susan Fowler. "Reflecting on One Very, Very Strange Year at Uber." Susan Fowler (blog). February 19, 2017. www.susanjfowler.com/blog/2017/2/19/reflecting-on-one-very-strange-year- at-uber. Accessed May 25, 2018.

- Rob Holdorp. "What 3 Million Lines of Code Means to a Piece of Luggage." IBM. 2:33. www.ibm.com/innovation/us/leadership/luggage/.

- Poul-Henning Kamp. "The Most Expensive One-Byte Mistake: Did Ken, Dennis, and Brian Choose Wrong with NUL-terminated Text Strings?" *ACM Queue*, July 25, 2011. queue.acm.org.

- Cade Metz, Ben Laffin, Hang Do Thi Duc, and Ian Clontz. "What Riding in a Self-Driving Tesla Tells Us About the Future of Autonomy." *New York Times,* November 14, 2022. https://www.nytimes.com/interactive/2022/11/14/technology/tesla-self-driving-flaws.html.

- Peter Robison. *Flying Blind: The 737 MAX Tragedy and the Fall of Boeing*. Doubleday, New York, NY, 2021.

- Charles Rotter. "Self-Driving Uber Running Red Light." YouTube, December 14, 2016. 0:30. www.youtube.com/watch?v=_CdJ4oae8f4.

- Viknesh Vijayenthiran. "Go for a Ride in Waymo's Self-Driving Car in This 360-Degree Video." Motor Authority (Web site), March 14, 2018. 3:36. https://www.motorauthority.com/news/1115747_go-for-a-ride-in-waymos- self-driving-car-in-this-360-degree-video.

Review Questions

1. What is the difference between an embedded system and a real-time system?
2. What is a race condition in software? Why are software race conditions difficult to debug?
3. Summarize the principal errors made by AECL throughout the life cycle of the Therac-25 linear accelerator.
4. The following reasons have been given for the failure of computerized systems:
5. a. A system designed for one purpose was used for another purpose.

   b. Software was used or reused without adequate testing.

   c. There was an error in storing or converting a data value.

   d. A line of code became a single point of failure.

   e. The overall system was too complicated to analyze.

   f. There was a software race condition.

   g. Too much responsibility for safety was put on human operator(s).

   h. There was another software error (other than those listed in a–g).

   For each of the following systems, select the principal reason or reasons why it failed to operate as specified.

- Patriot missile
  - Ariane 5
  - AT&T long-distance network
  - Mars Climate Orbiter
  - Mars Polar Lander
- Denver International Airport baggage system
  - Tokyo Stock Exchange
  - Direct-recording electronic voting machines
  - Therac-25
- Tesla Version 7.0 (Autopilot)
  - Boeing 737 MAX
  - Uber self-driving test vehicle

5. In your own words, define what it means for a computer system to be biased.

6. Define “algorithmic bias” in your own words.
7. Define “preexisting bias,” “technical bias,” and “emergent bias” in your own words.
8. What are the two principle causes of preexisting bias in AI decision-making systems?
9. In the context of machine learning, what is a proxy? Why are proxies problematic?
10. Define “demographic parity,” “equality of opportunity,” and “equalized odds” in your own words.
11. Summarize the challenges faced by designers attempting to create unbiased AI decision-making systems based on machine learning.

Discussion Questions

12. Have you ever been the victim of a software error? Whom did you blame? Now that you know more about the reliability of computer systems, do you still feel the same way?

13. Should an ecommerce site be required to honor the prices at which it offers and sells goods and services?

14. Should the FBI be responsible for the accuracy of information about criminals and crime victims it enters into the National Crime Information Center database?

15. Over a period of seven years, about 500 residents of Freeport, Texas, were overbilled for their water usage. Each resident paid on average about $170 too much, making the total amount of the overbillings about $100,000. The city council decided not to issue refunds, saying that about 300,000 bills would have had to be examined, some residents had left town, and

the individual refunds were not that large [**154**]. Did the city council make the right decision?

16. If a company sends a consumer an incorrect bill, should the company compensate the consumer for the time and effort the consumer takes to straighten out the mistake?

17. The chapter quotes NASA's project manager for the Mars Pathfinder as saying software hasn't improved in quality in the past 25 years. How could you determine whether software quality has improved in the past 25 years?

18. Should the US government ban the deployment of vehicles with SAE Level 3 automation?

19. Consider the Uber test-vehicle accident described in Section 8.7. How would you divide moral responsibility for the death among Uber's engineers and managers, the vehicle's safety operator, and the pedestrian?

20. In 2016 Florida became the first US state to pass legislation allowing fully autonomous vehicles (i.e., cars without a driver behind the steering wheel) to navigate public roads [**155**]. Are states being too "hands off"

when it comes to regulating autonomous-vehicle technology?

21. Suppose someone uses an app to summon from a taxi service a ride in an autonomous automobile. The taxi arrives, the customer gets in, and the car begins traveling to the desired destination. The customer is the only person in the taxi. Along the way, the taxi runs a red light and collides with a human-driven automobile that had the right of way. Who should be liable for the accident: the company that manufactured the vehicle, the taxi service, the customer, or someone else?

22. While waiting for an appointment with your physician, you see a brochure advertising a new surgical procedure that implants a tiny microprocessor inside your skull just behind your left ear. The purpose of the chip is to help you associate names with faces. The procedure for inserting the chip is so simple that your physician is performing it in his office. Suppose your career takes you into sales, where such a device could help you earn higher commissions. What questions would you want to have answered before you agreed to have such a device inserted into your skull?

In-Class Exercises

23. Debate the moral responsibility of three agents associated with the two Therac-25 overdoses occurring in Tyler, Texas: the radiation technician, the hospital director, and the programmer who wrote the code controlling the machine. Divide the class into six groups. Three groups (one for each of the three agents) should give reasons why their particular party should bear at least some of the moral responsibility for the deaths. The other three groups (one for each of the three agents) should give reasons why their particular party should not bear any moral responsibility.

24. California is working on an "intelligent highway" system that would allow computer-controlled automobiles to travel faster and closer together on freeways than today's human-controlled cars. What kinds of safety devices would have to be in such a system in order for you to feel comfortable using an intelligent highway? How many people in class would be comfortable being one of the first people to use the intelligent highway?

25. How many people in the class would ride on a computer-controlled airplane that did not have a human pilot on board?

26. Identify people in the class who have been beta testers for new software products. Ask them to tell the rest of the class about their experiences. What did acting as a beta tester teach them about software reliability?

27. A start-up company called Medick has been developing an exciting new product for handheld devices that will revolutionize the way nurses keep track of their hospitalized patients. The device will save nurses a great deal of time doing routine paperwork, reduce their stress levels, and enable them to spend more time with their patients.

    Medick's sales force has led hospital administrators to believe the product will be available next week as originally scheduled. Unfortunately, the software still contains quite a few bugs. All of the known bugs appear to be minor, but some of the planned tests have not yet been performed.

    Because of the fierce competition in the medical software industry, it is critical that this company be

the first to market. It appears a well-established company will release a similar product in a few weeks. If its product appears first, Medick will probably go out of business.

Divide the class into five groups representing the software engineers programming the device, the sales force that has been promoting the device, the managers of Medick, the venture capitalists who bankrolled Medick, and the nurses at a hospital purchasing the device. Each group should huddle to discuss the best course of action for Medick, and then the groups should take turns sharing their ideas with the rest of the class.

References

[1] Leslie Josephs. “Southwest Executive Tells Senate ‘We Messed Up’ in Holiday Travel Chaos.” *CNBC*, February 9, 2023. www.cnbc.com/2023/02/09/southwest-senate-hearing-holiday-meltdown.html.

[2] Chris Grygiel. “Starbucks Computer Outage: Early Closings or Free Coffee Across US, Canada.” Associated Press, April 24, 2015. www.charlotteobserver.com/news/business/article19447932.ht

[3] Dan Olds. “How One Bad Algorithm Cost Traders $440M.” *The Register*, August 3, 2012. www.theregister.co.uk/2012/08/03/bad_algorithm_lost_440_m

[4] Jennifer DiSabatino. “Unregulated Databases Hold Personal Data.” *Computerworld,* 36(4): 7, January 21, 2002.

[5] Peter G. Neumann. “More on False Arrests.” *Risks Digest,* 1(5), September 4, 1985.

[6] Rodney Hoffman. “NCIC Information Leads to Repeat False Arrest Suit.” *Risks Digest,* 8(71), May 17, 1989.

[7] Ted Bridis. “US Lifts FBI Criminal Database Checks.” Associated Press, March 25, 2003.

[8] Department of Justice, Federal Bureau of Investigation. “Privacy Act of 1974; Implementation.” *Federal Register,* 68(56): 60583–60586, March 24, 2003.

[9] “Computer Glitch Is to Blame for Faulty Bills, Qwest Says.” *Deseret News*, Salt Lake City, UT, July 24, 2001.

[10] “USDA Changes Livestock Price-Reporting Guidelines.” *Amarillo Globe-News*, July 24, 2001.

[11] “Software Error Returns Patent Office Mail.” *New York Times*, 75, August 9, 1996.

[12] Manny Fernandez. “Computer Error Caused Rent Troubles for Public Housing Tenants.” *New York Times*, August 5, 2009.

[13] “Calif. Computer Flub Lets Violent Prisoners Go Free.” *Seattle Times*, May 26, 2011.

[14] Ian MacKinnon and Stephen Goodwin. “Ambulance Chief Quits After Patients Die in Computer Failure.” *Independent*, London, October 29, 1992.

[15] "Flights at Japanese Airports Delayed." Associated Press, March 1, 2003.

[16] "LA County's Main Hospital Has Computer Breakdown, Delays Ensue." Associated Press, April 22, 2003.

[17] Daniel Michaels and Andy Pasztor. "Flight Check: Incidents Prompt New Scrutiny of Airplane Software Glitches." *Wall Street Journal*, 247(125), May 30, 2006.

[18] Nathaniel Popper. "The Stock Market Bell Rings, Computers Fail, Wall Street Cringes." *DealBook*, July 8, 2015. www.nytimes.com.

[19] Alan Yuhas. "Stock Trading Closed on NYSE after Glitch Caused Major Outage—as It Happened." *Guardian*, July 8, 2015. www.theguardian.com.

[20] Dan Kaplan. "Black Hat: Insulin Pumps Can Be Hacked." *SC Magazine*, August 4, 2011. www.scmagazine.com.

[21] Andy Greenberg. "Hackers Remotely Kill a Jeep on the Highway—with Me in It." *Wired*, July 21, 2015. www.wired.com.

[22] Aaron M. Kessler. “Fiat Chrysler Issues Recall over Hacking.” *New York Times*, July 24, 2015. www.nytimes.com.

[23] Robert Fry. “It’s a Steal: Bargain-Hunting or Barefaced Robbery?” *Times*, London, April 8, 2003.

[24] “Amazon Pulls British Site After iPaq Fire-Sale.” *NYtimes.com*, March 19, 2003.

[25] Victor L. Winter and Sourav Bhattacharya. Preface. In *High Integrity Software*, edited by Victor L. Winter and Sourav Bhattacharya, pp. xi–xiv. Kluwer Academic Publishers, Boston, MA, 2001.

[26] E. Marshall. “Fatal Error: How Patriot Overlooked a Scud.” *Science,* 255(5050): 1347, March 13, 1992.

[27] Jean-Marc Jézéquel and Bertrand Meyer. “Design by Contract: The Lessons of Ariane.” *Computer*, 30(1): 129–130, January 1997.

[28] J. L. Lions. “ARIANE 5: Flight 501 Failure, Report by the Inquiry Board.” European Space Agency, July 19, 1996. www.esa.int.

[29] Ivars Peterson. “Finding Fault: The Formidable Task of Eradicating Software Bugs.” *Science News*, 139(7): 104, February 16, 1991.

[30] Bruce Sterling. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Books, New York, NY, 1992.

[31] Jeff Foust. "Why Is Mars So Hard?" *Space Review*, June 2, 2003. www.thespacereview.com.

[32] Jet Propulsion Laboratory, California Institute of Technology. "NASA Facts: Mars Exploration Rover." October 2004. marsrover.jpl.nasa.gov.

[33] Richard de Neufville. "The Baggage System at Denver: Prospects and Lessons." *Journal of Air Transport Management*, 1(4): 229–236, December 1994.

[34] "Japan Court Upholds Lawsuit Against Tokyo Stock Exchange in $400M Error Case." *Japan Daily Press*, July 24, 2013. japandailypress.com.

[35] Tetsuo Tamai. "Social Impact of Information System Failures." *Computer,* 42(6): 58–65, June 2009.

[36] Stefan Lovgren. "Are Electronic Voting Machines Reliable?" *National Geographic News*, November 1, 2004. news.nationalgeographic.com.

[37] Jarrett Blanc. "Challenging the Norms and Standards of Election Administration: Electronic Voting." In

Challenging the Norms and Standards of Election Administration, pp. 11–19. International Foundation for Electoral Systems, Washington, DC, 2007.

[38] Sonia Arrison and Vince Vasquez. *Upgrading America's Ballot Box: The Rise of E-Voting*. 2nd ed. Pacific Research Institute, San Francisco, CA, 2006.

[39] "Electronic Ballots Fail to Win Over Wake Voters, Election Officials; Machines Provide Improper Vote Count at Two Locations." WRAL-TV (Raleigh-Durham, NC), November 2, 2002.

[40] Barbara Simons. "Electronic Voting Systems: The Good, the Bad, and the Stupid." *RFID,* 2(7): 20–26, October 2004.

[41] William Rivers Pitt. "Worse Than 2000: Tuesday's Electoral Disaster" (editorial). *Truthout*, November 8, 2004. www.Truth-out.org.

[42] Mark Johnson. "Winner So Far: Confusion." *Charlotte Observer*, November 5, 2004.

[43] Charles Rabin and Darran Simon. "Glitches Cited in Early Voting: Early Voters Are Urged to Cast Their Ballots with Care Following Scattered Reports of

Problems with Heavily Used Machines." *Miami Herald*, October 28, 2006.

[44] "Florida Candidate Disputes Election Results." CNN.com, December 20, 2006.

[45] Marc Caputo and Gary Fineout. "New Tests Fuel Doubts About Vote Machines." *Miami Herald*, December 15, 2005.

[46] Jeremy Epstein. "Weakness in Depth: A Voting Machine's Demise." *IEEE Security & Privacy*, 55–58, May/June 2015.

[47] "Transparent Liberty, Accountable Election Systems" (leaflet). Open Voting Consortium. www.openvoting.org.

[48] Cheryl Gerber. "Voting 2.0." *Chronogram*, 22–26, January 2006.

[49] Pacific Research Institute. "More E-Voting Red Tape Threatens Ballot Booth Benefits, New Study Says" (press release). October 31, 2006.

[50] Matt Zdun. "Machine Politics: How America Casts and Counts Its Votes." *Reuters*, August 23, 2022. www.reuters.com/graphics/USA-ELECTION/VOTING/mypmnewdlvr/.

[51] Nancy Leveson and Clark Turner. "An Investigation of the Therac-25 Accidents." *Computer*, 26(7): 18–41, 1993.

[52] Walt Bogdanich. "Radiation Offers New Cures, and Ways to Do Harm." *New York Times*, January 23, 2010. www.nytimes.com.

[53] Ryan Bradley. "Tesla Autopilot: The Electric-Vehicle Maker Sent Its Cars a Software Update That Suddenly Made Autonomous Driving a Reality." *MIT Technology Review*, 119(2): 62–65, March/April 2016.

[54] "Your Autopilot Has Arrived." Tesla Motors (blog), October 14, 2015. www.tesla.com/blog/your-autopilot-has-arrived.

[55] SAE International. "Automated Driving: Levels of Driving Automation Are Defined in New SAE International Standard J3016." 2014. www.sae.org/misc/pdfs/automated_driving.pdf.

[56] Rachel Abrams and Annalyn Kurtz. "Joshua Brown, Who Died in Self-Driving Accident, Tested Limits of His Tesla." *New York Times*, July 1, 2016.

[57] Joshua Brown. "Tesla Autopilot v7.0 Intro Video." YouTube, October 15, 2015.

www.youtube.com/watch?v=mTZD7GFV6H4.

[58] Joshua Brown. “Tesla v7.0 Autopilot: Showing When It Can’t Handle It.” YouTube, October 18, 2015. www.youtube.com/watch?v=GaIbu7K90CA.

[59] Joshua Brown. “Tesla v7.0 Autopilot: Very Difficult RR Track Turn.” YouTube, October 18, 2015. www.youtube.com/watch?v=Sb1y2z7SKhk.

[60] Mark Gillispie and John Seewer. “Tesla Driver Killed While Using Autopilot Loved Fast Cars.” Associated Press, July 1, 2016.

[61] Anjali Singhvi and Karl Russell. “Inside the Self-Driving Tesla Fatal Accident.” *New York Times*, July 12, 2016.

[62] Joseph A. Gregor. “Driver Assistance System: Specialist’s Factual Report.” National Transportation Safety Board, March 7, 2017.

[63] David Shepardson. “U.S. Regulator Finds No Evidence of Defects After Tesla Death Probe.” *Reuters*, January 19, 2017. www.reuters.com/article/us-tesla-safety-idUSKBN1532F8.

[64] Fred Lambert. “Tesla Elaborates on Autopilot’s Automatic Emergency Braking Capacity over Mobileye’s System.” *electrek*, July 2, 2016.

electrek.co/2016/07/02/tesla-autopilot-mobileye-automatic-emergency-braking/.

[65] Alex Davies. “Ford’s Skipping the Trickiest Thing About Self-Driving Cars.” *Wired*, November 10, 2015.

[66] Alex Davies. “The Very Human Problem Blocking the Path to Self-Driving Cars.” *Wired*, January 1, 2017.

[67] Electrek.co. “Tesla Model S Driver Caught Sleeping at the Wheel While on Autopilot Electrek.” YouTube, May 23, 2016.

[68] Robert Squire. “Technical Reconstruction Group Chairman’s Factual Report: Williston, FL, HWY16FH018.” National Transportation Safety Board, 2017.

[69] David Shepardson. “Tesla Driver in Fatal ‘Autopilot’ Crash Got Numerous Warnings: U.S. Government.” *Reuters*, June 20, 2017.

[70] Jack Stewart. “Tesla’s Self-Driving Software Gets a Major Update.” *Wired*, September 11, 2016.

[71] Will Oremus. “The Paradox of the Self-Driving Car.” *Slate*, November 12, 2015.

[72] Samuel Gibbs. “Elon Musk: Tesla Cars Will Be Able to Cross US with No Driver in Two Years.” *Guardian*, January 11, 2016.

[73] Alexandria Sage and David Ingram. “Tesla Mixes Warnings and Bravado About Hands-Free Driving.” *Reuters*, July 1, 2016. www.reuters.com/article/us-tesla-autopilot-drivers-idUSKCN0ZH64O.

[74] Biz Carson. “Travis Kalanick on Uber’s Bet on Self-Driving Cars: ‘I Can’t Be Wrong.’” *Business Insider*, August 18, 2016. www.businessinsider.com/travis-kalanick-interview-on-self-driving-cars-future-driver-jobs-2016-8.

[75] Josh Lowensohn. “Uber Gutted Carnegie Mellon’s Top Robotics Lab to Build Self-Driving Cars.” *Verge*, May 19, 2015. www.theverge.com/transportation/2015/5/19/8622831/uber-self-driving-cars-carnegie-mellon-poached.

[76] Signe Brewster. “Uber Starts Self-Driving Car Pickups in Pittsburgh.” *TechCrunch*, September 14, 2016. techcrunch.com/2016/09/14/1386711/.

[77] “San Francisco, Your Self-Driving Uber Is Arriving Now.” Uber (press release), December 14, 2016.

newsroom.uber.com/san-francisco-your-self-driving-uber-is-arriving-now/.

[78] Joe Fitzgerald Rodriguez. “Video Appears to Show Uber Self-Driving Car Running Red Light in SF.” *San Francisco Examiner*, December 14, 2016. www.sfexaminer.com/uber-self-driving-vehicle-appears-launch-red-light-first-day-sf/.

[79] Doug Ducey. “AZ Welcomes Uber!” (tweet), December 22, 2016. twitter.com/dougducey/status/812063724697567238.

[80] Daisuke Wakabayashi. “Uber’s Self-Driving Cars Were Struggling Before Arizona Crash.” *New York Times*, March 23, 2018. www.nytimes.com/2018/03/23/technology/uber-self-driving-cars-arizona.html?smid=tw-share.

[81] Laura Bliss. “Former Uber Backup Driver: ‘We Saw This Coming.’” *CityLab*, March 27, 2018. www.citylab.com/transportation/2018/03/former-uber-backup-driver-we-saw-this-coming/556427/.

[82] Shigeru Haga. “An Experimental Study of Signal Vigilance Errors in Train Driving.” *Ergonomics*, 27: 755–765, 1984.

[83] James F. O'Hanlon. "Boredom: Practical Consequences and a Theory." *Acta Psychologica*, 49(1): 53–82, 1981.

[84] M. L. Cummings, C. Mastracchio, J. M. Thornburg, and A. Mkrtchyan. "Boredom and Distraction in Multiple Unmanned Vehicle Supervisory Control." *Interacting with Computers*, 25(1): 34–47, 2013.

[85] Matthew B. Weinger. "Vigilance, Boredom, and Sleepiness." *Journal of Clinical Monitoring and Computing*, 15(7–8): 549–552, 1999.

[86] Amy Martyn. "Autonomous Car Companies Report Getting Rear-Ended in Most Crashes, Blame Driver Error." *Consumer Affairs*, October 20, 2017. www.consumeraffairs.com/news/autonomous-car-companies-report-getting- rear-ended-in-most-crashes-blame-driver-error-102017.html.

[87] Aarian Marshall. "False Positives: Self-Driving Cars and the Agony of Knowing What Matters." *Wired*, May 29, 2018. www.wired.com/story/self-driving-cars-uber-crash-false-positive-negative/.

[88] Aarian Marshall and Alex Davies. "Uber's Self-Driving Car Saw the Woman It Killed, Report Says, Wired, May

24, 2018." www.wired.com/story/uber-self-driving-crash-arizona-ntsb-report/.

[89] National Transportation Safety Board. "Preliminary Report Highway HWY18MHH010." May 24, 2018. www.ntsb.gov/investigations/AccidentReports/Reports/HWY1 prelim.pdf.

[90] Troy Griggs and Daisuke Wakabayashi. "How a Self-Driving Uber Killed a Pedestrian in Arizona." *New York Times*, March 21, 2018.

[91] Heather Somerville and David Shepardson. "Uber Driver Was Streaming Hulu Show Just Before Self-Driving Car Crash—Police Report." *Reuters*, June 21, 2018. www.reuters.com/article/uber-selfdriving-crash/uber-driver-was- streaming-hulu-show-just-before-self-driving-car-crash-police-report-idUSL1N1TO05R.

[92] Melissa Daniels. "Arizona Governor Suspends Uber from Autonomous Testing." Associated Press. March 26, 2018. www.usnews.com/news/technology/articles/2018-03-26/arizona-governor- suspends-uber-from-autonomous-testing.

[93] Ryan Randazzo. “Uber Shutting Down Self-Driving Operations in Arizona After Fatal Crash.” *The Republic*, May 23, 2018. www.azcentral.com/story/news/local/tempe-breaking/2018/05/23/uber-close- self-driving-operations-arizona/636974002/.

[94] Loren Thompson. “How Boeing Got Here: It’s Not the Story You Have Been Hearing Lately.” *Forbes*, May 20, 2019.

[95] Justin Hayward, “The Battle of the Big Planes: Why Airbus and Boeing Won the Race.” *Simple Flying,* September 24, 2020.

[96] Javier Mediavilla. “Boeing 737 Vs Airbus A320 Family Deliveries, 1967–2018.” *The Blog by Javier,* January 24, 2019. https://theblogbyjavier.com/2019/01/24/boeing-737-vs-airbus-a320-family-deliveries-1967-2018/.

[97] Peter Robison. *Flying Blind: The 737 MAX Tragedy and the Fall of Boeing*. Doubleday, New York, 2021.

[98] “Final Committee Report: The Design, Development & Certification of the Boeing 737 MAX.” The House

Committee on Transportation & Infrastructure. September 2020.

[99] Peter Sanders and Doug Cameron. "Boeing Confident on 787 Deliveries This Year." *Wall Street Journal,* January 26, 2011.

[100] David Gelles, Natalie Kitroeff, Jack Nicas, and Rebecca R. Ruiz. "Boeing Was 'Go, Go, Go' to Beat Airbus with the 737 MAX." *New York Times,* March 23, 2019. https://www.nytimes.com/2019/03/23/business/boeing-737-max-crash.html.

[101] Steve Wilhelm. "What's the ROI for Boeing 737 Replacement?" *Puget Sound Business Journal,* July 5, 2011. https://www.bizjournals.com/seattle/blog/2011/07/whats-the-roi-for-boeing-737.html.

[102] Mark Bailey and Keven McAlester. "Downfall: The Case Against Boeing." *Netflix,* February 18, 2022. 89 minutes.

[103] Nicola Clark. "Jet Order by American Is a Coup for Boeing's Rival." *New York Times,* July 20, 2011. https://www.nytimes.com/2011/07/21/business/global/americar places-record-order-with-2-jet-makers.html.

[104] "Boeing, Lion Air Announce Historic Commitment For up to 380 737s." The Boeing Company press release, November 17, 2011. https://boeing.mediaroom.com/2011-11-17-Boeing-Lion-Air-Announce- Historic-Commitment-for-up-to-380-737s.

[105] Dominic Gates and Mike Baker. "The Inside Story of MCAS: How Boeing's 737 MAX System Gained Power and Lost Safeguards." *The Seattle Times,* June 22, 2019. Updated June 24, 2019. https://www.seattletimes.com/seattle-news/times-watchdog/the-inside- story-of-mcas-how-boeings-737-max-system-gained-power-and-lost- safeguards/.

[106] Seattle Times staff. "Two Tragic Flights, 12 Problems." *The Seattle Times,* October 28, 2019.

[107] "Timeline of Activities Leading to the Certification of the Boeing 737 MAX 8 Aircraft and Actions Taken After the October 2018 Lion Air Accident." FAA Report No. AV2020037. Office of the Inspector General, US Department of Transportation. June 29, 2020. https://www.oig.dot.gov/sites/default/files/FAA%20Oversight%20of%20Boeing%020737%20MAX%20C

[108] Jack Nicas, Natalie Kitroeff, David Gelles, and James Glanz. "Boeing Built Deadly Assumptions into 737 MAX, Blind to a Late Design Change." *New York Times,* June 1, 2019. https://www.nytimes.com/2019/06/01/business/boeing-737-max-crash.html.

[109] Curt Devine and Drew Griffin. "Boeing Relied on Single Sensor for 737 MAX That Had Been Flagged 216 Times to FAA." *CNN,* April 30, 2019. https://www.cnn.com/2019/04/30/politics/boeing-sensor-737-max-faa/index.html

[110] "Final KNKT.18.10.35.04 Aircraft Accident Investigation Report: PT. Lion Mentari Airlines, Boeing 737-8 (MAX); PK-LQP, Tanjung Karawang, West Java, Republic of Indonesia, 29 October 2018." Komite Nasional Keselamatan Transportasi, Republic of Indonesia. October 2019.

[111] "Uncommanded Nose Down Stabilizer Trim Due to Erroneous Angle of Attack (AOA) During Manual Flight Only." Flight Crew Operations Manual Bulletin for The Boeing Company, No. TBC-19. November 6, 2018. https://www.extracrew.com/wp-

content/uploads/2018/11/TBC-19-Uncommanded-Nose-Down-Stab-Trim-Due-to-AOA.pdf.

[112] "Boeing Statement on Lion Air Flight 610 Preliminary Report." Press Release. The Boeing Company. November 27, 2018. https://boeing.mediaroom.com/news-releases-statements?item=130336.

[113] "Investigation Report on Accident to the B737-MAX8 Reg. ET-AVJ Operated by Ethiopian Airlines, 10 March, 2019." The Federal Democratic Republic of Ethiopia Ministry of Transport and Logistics. December 2022. https://www.havkom.se/assets/reports/L-34_19-No-AI_01_18-ACCIDENT-FINAL-REPORT_compressed.pdf.

[114] Danny Lee. "European Union Grounds Boeing 737 MAX, as a Growing Cascade of Nations Follows China's Lead After Deadly Crashes." *South China Morning Post,* March 12, 2019. https://www.scmp.com/news/hong-kong/hong-kong-economy/article/3001179/ singapore-joins-growing-list-countries-grounding.

)

[115] "Summary of the FAA's Review of the Boeing 737 MAX: Return to Service of the Boeing 737 MAX Aircraft." *Federal Aviation Administration,* November 18, 2020. https://www.faa.gov/foia/electronic_reading_room/boeing_reac

[116] Chris Isidore. "Boeing Agrees to Pay $2.5 Billion to Settle Charges It Defrauded FAA on 737 Max." *CNN,* January 8, 2021. https://www.cnn.com/2021/01/07/business/boeing-737-max-faa-fraud/index.html.

[117] David Gelles. "Boeing Expects 737 Max Costs Will Surpass $18 Billion." *New York Times,* January 29, 2020. https://www.nytimes.com/2020/01/29/business/boeing-737-max-costs.html.

[118] David Shepardson. "U.S. Attorney General to Meet with Boeing 737 MAX Crash Victims' Relatives." *Reuters,* January 20, 2022. https://www.reuters.com/business/aerospace-defense/us-attorney-general- meet-with-boeing-737-max-crash-victims-relatives-2022-01-20/.

[119] Edith Carli. "How Do Human Weaknesses Complicate Decision Making?" Center for Genius Authoritative

Answers (Web site), June 4, 2022. https://www.cgaa.org/article/how-do-human-weaknesses-complicate- decision-making.

[120] Ben Demers. "Where AI Can Save Businesses the Most Money." *Kiplinger,* April 19, 2023. https://www.kiplinger.com/personal-finance/where-ai-can-save-businesses-the-most-money.

[121] Batya Friedman and Helen Nissenbaum. "Bias in Computer Systems." *ACM Transactions on Information Systems,* 14(3): 330–347, July 1996.

[122] Steve Lohr. "Facial Recognition Is Accurate, If You're a White Guy." *New York Times,* February 9, 2018. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[123] Brian Dean. "Here's What We Learned About Organic Click Through Rate." Backlinko (Web site), October 14, 2022. https://backlinko.com/google-ctr-stats.

[124] Ayush Jalan. "6 Lessons Microsoft Learned from Its Tay AI Chatbot Disaster." Make Use Of (Web site), May 10, 2023. https://www.makeuseof.com/lessons-microsoft-learned-tay-ai-disaster/.

[125] Peter Lee. “Learning from Tay’s Introduction.” *Official Microsoft Blog,* March 25, 2016. https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/.

[126] Nico Grant and Kashmir Hill. “Google’s Photo App Still Can’t Find Gorillas. and Neither Can Apple’s.” *New York Times,* May 22, 2023. https://www.nytimes.com/2023/05/22/technology/ai-photo-labels-google-apple.html.

[127] Tom Simonite. “Machines Taught by Photos Learn a Sexist View of Women.” *Wired,* August 21, 2017. www.wired.com/story/machines-taught-by-photos-learn-a-sexist-view-of-women/.

[128] Jieyu Zhao, Tianlu Wang, Mark Yatskar, Vicente Ordonez, and Kai-Wei Chang. “Men Also Like Shopping: Reducing Gender Bias Amplication Using Corpus-Level Constraints.” *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing,* January 2017. www.aclweb.org/anthology/D17-1323.

[129] Allison Koenecke, Andrew Nam, Emily Lake, Joe Nudell, Minnie Quartey, Zion Mengesha, Connor Toups, John R. Rickford, Dan Jurafsky, and Sharad

Goel. “Racial Disparities in Automated Speech Recognition.” *Proceedings of the National Academy of Science of the United States of America*, 117(14): 7684–7689, March 23, 2020. https://www.pnas.org/doi/10.1073/pnas.1915768117.

[130] Melanie Evans and Anna Wilde Mathews. “New York Regulator Probes UnitedHealth Algorithm for Racial Bias; Financial Services Department Is Investigating Whether Algorithm Violates State Antidiscrimination Law.” *Wall Street Journal,* October 26, 2019.

[131] Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. “Dissecting Racial Bias in an Algorithm Used to Managed the Health of Populations.” *Science,* 366(6464): 447–453.

[132] “Wealth Gaps Rise to Record Highs Between Whites, Blacks, Hispanics.” *Pew Research Center,* July 26, 2011. https://www.pewresearch.org/social-trends/2011/07/26/wealth-gaps-rise- to-record-highs-between-whites-blacks-hispanics/.

[133] Candace Jackson. “What Is Redlining?” *New York Times,* August 17, 2021. https://www.nytimes.com/2021/08/17/realestate/what-is-redlining.html.

[134] Rashawn Ray, Andre M. Perry, David Harshbarger, Samantha Elizondo, and Alexandra Gibbons. "Homeownership, Racial Segregation, and Policy Solutions to Racial Wealth Equality." Brookings Institution, September 1, 2021. https://www.brookings.edu/essay/homeownership-racial-segregation-and- policies-for-racial-wealth-equity/.

[135] Dettling, Lisa J., Joanne W. Hsu, Lindsay Jacobs, Kevin B. Moore, and Jeffrey P. Thompson. "Recent Trends in Wealth-Holding by Race and Ethnicity: Evidence from the Survey of Consumer." Finances. *The Federal Reserve,* September 27, 2017. https://www.federalreserve.gov/econres/notes/feds-notes/recent-trends- in-wealth-holding-by-race-and-ethnicity-evidence-from-the-survey-of- consumer-finances-20170927.htm.

[136] Edmund L. Andrews. "How Flawed Data Aggravates Inequality in Credit Scores." Insights by Stanford Business (Web site), August 24, 2021. https://www.gsb.stanford.edu/insights/how-flawed-data-aggravates- inequality-credit-scores.

[137] Laura Blattner and Scott Nelson. "How Costly Is Noise? Data and Disparities in Consumer Credit," May 5, 2021. https://arxiv.org/pdf/2105.07554.pdf.

[138] Albert Meijer and Martijn Wessels. "Predictive Policing: Review of Benefits and Drawbacks." *International Journal of Public Administration,* 42(12): 1031–1039, 2019. https://doi.org/10.1080/01900692.2019.1575664.

[139] Erinn Figg. "The Legacy of Blue CRUSH." *High Ground,* March 19, 2014. https://www.highgroundnews.com/features/BlueCrush031214.

[140] Zach Friend. FBI Law Enforcement Bulletin, April 9, 2013. https://leb.fbi.gov/articles/featured-articles/predictive-policing- using-technology-to-reduce-crime.

[141] Duncan Purves. "Fairness in Algorithmic Policing." *Journal of the American Philosophical Association,* 741–761, 2022. https://www.cambridge.org/core/journals/journal-of-the-american- philosophical-association/article/fairness-in-algorithmic-policing/A93BD2FBA25DEDBC6620B25D1C9A8A26.

[142] Leia Miller. “LAPD Will End Controversial Program That Aimed to Predict Where Crimes Would Occur.” *Los Angeles Times*, April 21, 2020. https://themarkup.org/prediction-bias/2021/12/02/crime-prediction- software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[143] Kristi Sturgill. “Santa Cruz Becomes the First U.S. City to Ban Predictive Policing.” *Los Angeles Times*, June 26, 2020. https://www.latimes.com/california/story/2020-06-26/santa-cruz-becomes- first-u-s-city-to-ban-predictive-policing.

[144] “Reduce Major Violent Crime.” Memphis Data Hub (Web site). https://data.memphistn.gov/stories/s/Reduce-Major-Violent-Crime/t495- sd4v/. Accessed May 12, 2023.

[145] “What Is EBDM?” National Institute of Corrections. https://info.nicic.gov/ebdm/. Accessed April 29, 2023.

[146] Jeff Larson, Surya Mattu, Lauren Kirchner, and Julian Angwin. “How We Analyzed the COMPAC Recidivism Algorithm.” *ProPublica*, May 23, 2016.

https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

[147] William Dieterich, Christina Mendoz, and Tim Brennan. “COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity: Performance of the COMPAS Risk Scales in Broward County.” Northpoint Inc. Research Department, July 8, 2016. https://www.documentcloud.org/documents/2998391-ProPublica-Commentary- Final-070616.html.

[148] Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan. “Inherent Trade-Offs in the Fair Determinations of Risk Scores,” arXiv:1609.05807v2 [cs.LG] November 17, 2016.

[149] “Putting Principles into Practice at Microsoft.” Web page. https://www.microsoft.com/en-us/ai/our-approach? activetab=pivot1%3aprimaryr5. Accessed May 18, 2023.

[150] “Responsibility: Our Principles.” Web page. https://ai.google/responsibility/principles/. Accessed May 18, 2023.

[151] Aaron Williams and Armand Emamdjomeh. “America Is More Diverse than Ever—But Still Segregated.” *Washington Post,* May 10, 2018.

https://www.washingtonpost.com/graphics/2018/national/segre
us-cities/.

[152] Daniel Schwarcz and Anya E. R. Prince. "Proxy Discrimination in the Age of Artificial Intelligence and Big Data." *Iowa Law Review*, 105: 1257–1318, 2020 https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1695&context=faculty_articles.

[153] "Machine Learning Glossary." Google for Developers (Web site). https://developers.google.com/. Accessed July 12, 2023.

[154] "Texans Get Soaked." *IEEE Software*, 14(5): 114, September/October 1997.

[155] Michael J. Coren. "How Florida Became the Most Important US State in the Race to Legalize Self-Driving Cars." *Quartz*, September 20, 2016. qz.com/781113/howflorida- became-the-most-important-state-in-the-race-to-legalize-self-driving-cars/.

Chapter 9

Professional Ethics

9.1 Introduction

JACOBUS LENTZ WAS THE NETHERLANDS' INSPECTOR OF POPULATION registries before World War II. In this role he managed a well-oiled data-processing infrastructure using machines leased from IBM, and he reveled in the collection of personal data, writing: "Theoretically, the collection of data for each person can be so abundant and complete, that we can finally speak of a paper human representing the natural human" [**1**, p. 304].

Lentz devised a forgery-proof identification card and advocated that every citizen be required to get one and carry it at all times, but the Dutch government rejected his proposal; it offended democratic sensibilities. When the Netherlands came under German occupation in 1940, Lentz got another opportunity to promote his invention. He shared his design with the Nazis, who were impressed; it was far superior to the identification card being used in Germany. Soon the identification card designed by Lentz was issued to everyone in the Netherlands.

In January 1941 the German occupiers began a special census of Jewish people in the Netherlands. All Jewish people were

required to register at their local census office. There was widespread condemnation of this edict across Dutch society, but the Jewish people complied. The penalty for failing to register was five years in prison and the loss of one's property. Besides, those who failed to register could be tracked down because the government had up-to-date information about them that was gathered when the Lentz identification cards were issued.

Lentz did not simply comply with the directives of the Germans, he anticipated their needs. When they contacted him in May 1941 about producing an alphabetical register of the Jewish population, Lentz replied that his office had already begun setting up a system to do just that. In his memoirs Lentz wrote, "I rented a Hollerith installation with which the professional statistical survey has been composed, which satisfied the Germans very much, and gave them the convictions that my opinions had been correct" [**1**, p. 312].

In July 1942 twice-weekly trains began deporting Jewish people from the Netherlands to concentration camps in Eastern Europe. The alphabetized lists provided by Lentz's office allowed the Germans to conduct this operation with great efficiency: rounding up Jewish people in an orderly fashion and keeping the trains running on schedule. Of the

140,000 Jewish people in the Netherlands at the time of the German invasion, 107,000 were deported, and of these 102,000 died [**1**].

Informally, a **profession** is a vocation that requires a high level of education and practical experience in the field. Professionals have a special obligation to ensure their actions are for the good of those who depend on them, because their decisions can have more serious consequences than the choices made by those holding less responsible positions in society. Jacobus Lentz had great expertise in the world of data processing. As inspector of population registries, he was in a position of great responsibility. Sadly, he focused on demonstrating his creativity, technical abilities, and industriousness and ignored the consequences of his actions. Lacking a moral compass, he allowed himself to play an important role in the Nazis' plan for genocide.

In this chapter we focus on moral decisions made by people who design, implement, operate, or maintain computer hardware or software systems. We begin by considering the extent to which a computer-related career is a profession along the lines of medicine or law. Next we present and analyze a code of ethics for an important computer-related discipline: software engineering. Four case studies give us the

opportunity to use the software engineering code of ethics as a tool for ethical analysis.

Computer professionals also have moral obligations related to their coworkers. Women and people of color are significantly underrepresented in the computing field. We examine the benefits of creating a more diverse workplace, discuss actions that all computer professionals can take to help create a more inclusive environment, and share best practices of organizations that have improved their diversity, equity, and inclusion.

Finally, we discuss whistle-blowing: a situation in which a member of an organization breaks ranks to reveal actual or potential harm to the public. Whistle-blowing raises important moral questions about loyalty, trust, and responsibility. Two accounts of whistle-blowing illuminate these moral questions and demonstrate the personal sacrifices some have made for the greater good of society. We consider the important role management plays in creating an organizational atmosphere that either allows or suppresses internal dissent.

9.2 How Well Developed Are the Computing Professions?

Millions of people have a computer-related job title, such as computer engineer, computer scientist, programmer, software engineer, system administrator, or systems analyst. Is a computer-related career a fully developed profession like medicine or law? Let's consider the characteristics of a fully developed profession.

9.2.1 Characteristics of a Fully Developed Profession

A fully developed profession has a well-organized infrastructure for certifying new members and supporting those who already belong to the profession. Ford and Gibbs

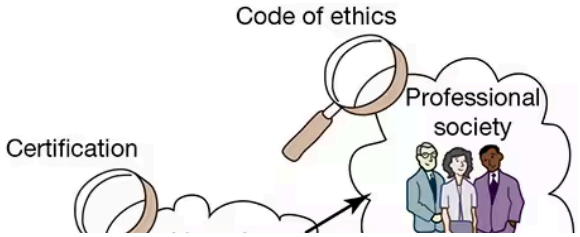
have identified eight components of a mature professional infrastructure:[1]

- *Initial professional education*—formal course work completed by candidates before they begin practicing the profession
- *Accreditation*—a means of assuring that the formal course work meets the standards of the profession
- *Skills development*—activities that provide candidates with the opportunity to gain practical skills needed to practice the profession
- *Certification*—a process by which candidates are evaluated to determine their readiness to enter the profession
- *Licensing*—the process giving candidates the legal right to practice the profession
- *Professional development*—formal course work completed by professionals in order to maintain and develop their knowledge and skills
- *Code of ethics*—a mechanism by which a profession ensures that its members use their knowledge and skills for the benefit of society

- *Professional society*—an organization promoting the welfare of the profession, typically consisting of most, if not all, members of the profession

Figure 9.1 illustrates how these components work together to support the profession. A person desiring to join the profession undertakes some initial professional education. A process of accreditation assures that the educational process is sound. After completing their formal education, candidates gain skills through practical experience working in the field. Another check determines if the candidate is ready to be certified. Successful candidates are licensed to practice the profession.

Figure 9.1



When the public can trust the competence and integrity of the members of a profession, every one of its members benefits. For this reason professionals have a stake in ensuring that fellow members of the profession are capable and act appropriately. For mature professions, professional societies establish codes of ethics and require their members to keep their knowledge current through continuing education and training. Professionals who do not follow the code of ethics or fail to keep up with changes in the field can lose their licenses.

9.2.2 Case Study: Certified Public Accountants

To illustrate these steps, let's consider how a person becomes a certified public accountant (CPA). We choose accounting because it is a fully developed profession that does not require graduate study for membership. In this respect it is more similar to a typical computer-related career than the medical or legal professions, which require their members to earn advanced degrees.

The first step for someone wishing to become a CPA is to graduate with 150 semester credit hours and at least a bachelor's degree from an accredited college or university. Many people pursuing a CPA choose to major in accounting, although it is not strictly necessary. However, the candidate must have completed at least 24 semester credit hours in accounting, auditing, business law, finance, and tax subjects. After graduation, the candidate gets practical training in the profession by finding employment as an accountant working under the supervision of a CPA. Finally, candidates must sit for the CPA exam, which has four sections. Candidates who do not pass at least two parts must retake the entire exam. Candidates who pass at least two parts of the exam must pass the remaining parts within five years.

Completion of the necessary formal education, plus satisfactory scores on every section of the CPA exam, plus two years' work experience enable an accountant to become a certified public accountant. In order to retain certification, CPAs must fulfill continuing education requirements and abide by the profession's code of ethics.

9.2.3 How Do Computer-Related Careers Stack Up?

It is easy to find a crucial difference between systems analysts, computer programmers, and system administrators on the one hand and accountants, lawyers, and physicians on the other hand. At the heart of every mature profession is certification and licensing. Certification and licensing allow a profession to determine who will be allowed to practice the profession. For example, a person may not practice law in a state without passing the bar exam and being granted a license. In contrast, people may write computer programs and maintain computer systems, either as consultants, sole proprietors, or members of larger firms, without being certified or having been granted a license.

There are other differences between computer-related careers and mature professions. A person does not have to complete college or serve an apprenticeship under the guidance of an experienced mentor in order to gain employment as a programmer, system administrator, or systems analyst. The vast majority of people who hold computer-related jobs do not belong to either of computing's professional societies. It is up to particular employers to monitor the behavior of their employees and guide their continuing education—no professional organization has the authority to forbid

someone from managing computer networks or writing computer programs.

In another important respect computer programmers differ from most professionals, such as dentists and ministers. Typically, professionals work directly with individual clients. A dentist treats one patient at a time. An accountant audits one business at a time. Most computer programmers work inside a company as part of a team that includes many other programmers as well as managers. In this environment the responsibility of an individual person is difficult to discern. Low-level technical decisions are made by groups, and final authority rests with management.

Status of Certification and Licensing

A **software engineer** is someone engaged in the development or maintenance of software, or someone who teaches in this area. A path to certification and licensing of software engineers in the United States was attempted; it was similar to the path taken by engineers in other disciplines, such as civil engineering and mechanical engineering. In order to become licensed, engineers were required to gain four years of post-college work experience and pass two examinations: the Fundamentals of Engineering (FE) examination and a discipline-specific Principles and Practice of Engineering

examination (often called the PE exam). The National Council of Examiners for Engineering and Surveying (NCEES) is responsible for developing and administering the FE and PE examinations.

The NCEES partnered with the professional organization IEEE-USA to develop a PE exam for software, and it offered the exam for the first time in 2013. However, only 81 people took the exam in the first five years, and in 2018 the NCEES board of directors voted to discontinue the exam after offering it one last time in April 2019 [3].

Ability to Harm the Public

The computing "profession" may not be as well developed as the medical or legal professions, but in one key respect—the ability to harm members of the public—those who design, implement, and maintain computer hardware and software systems sometimes hold responsibilities similar to those held by members of mature professions. The Therac-25 killed or gravely injured at least six people, in part because of defective software. An overly powerful Maneuvering Characteristics Augmentation System contributed to two fatal crashes of the Boeing 737 MAX that killed 346 people. While most software engineers do not write code for safety-critical systems such as linear accelerators, commercial jetliners, or

self-driving automobiles, society does depend on the quality of their work. People make important business decisions based on the results they get from their spreadsheet programs. Millions rely upon commercial software to help them produce their income-tax returns. Errors in programs can result in such harms as lost time, incorrect business decisions, and fines. System administrators are responsible for keeping computer systems running reliably without infringing on the privacy of the computer users.

The ability to cause harm to members of the public is a powerful reason why those in computer-related careers must act according to ethical principles. Without formal certification and licensing and other components of a well-developed profession to rely upon, those in computer-related careers must take more personal responsibility for developing their ethical decision-making skills.

One important decision-making skill to develop is the ability to avoid the temptation to rationalize bad behavior. Another skill is the ability to apply the viable ethical theories presented in Chapter 2. Kantianism, utilitarianism, social contract theory, and virtue ethics all contain important insights into what it means to do the right thing. A third important decision-making skill to develop is the ability to

apply the Software Engineering Code of Ethics and Professional Practice, endorsed by both the ACM and the IEEE-CS.

om Gary Ford and Norman E. Gibbs, “A Mature Profession of Software ıgineering.” Technical report, Carnegie Mellon University, January 1996.

ɔpyright © 1996 Carnegie Mellon University. All rights reserved.

9.3 Software Engineering Code of Ethics

The Software Engineering Code of Ethics and Professional Practice is a practical framework for moral decision making related to problems that software engineers may encounter.

The Software Engineering Code of Ethics and Professional Practice is reproduced here in its entirety [4].

Preamble

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do

good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policymakers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer's humanity, in special care owed to people affected by the work of software engineers, and the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission.

The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings with due respect; to consider how the public, if reasonably well informed, would view their decisions; to analyze how the least empowered will be affected by their decisions; and to consider whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for the health, safety and welfare of the public is primary; that is, the “Public Interest” is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

Principles

Principle 1: Public

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as

appropriate:

1.01 Accept full responsibility for their own work.

1.02 Moderate the interests of the software engineer, the employer, the client and the users with the public good.

1.03 Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good (Figure 9.2).

Figure 9.2

Software engineers shall approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy, or harm the environment. The ultimate effect of the work should be to the public good (clause 1.03).

1.04 Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05 Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

1.06 Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

1.07 Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.

1.08 Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

Principle 2: Client and Employer

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the

public interest. In particular, software engineers shall, as appropriate:

2.01 Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02 Not knowingly use software that is obtained or retained either illegally or unethically (Figure 9.3).

Figure 9.3

Software engineers shall not knowingly use software that is obtained or retained either illegally or unethically (clause 2.02).

2.03 Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.

2.04 Ensure that any document upon which they rely has been approved, when required, by someone authorized

to approve it.

2.05 Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06 Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07 Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.

2.08 Accept no outside work detrimental to the work they perform for their primary employer.

2.09 Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

Principle 3: Product

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01 Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.

3.02 Ensure proper and achievable goals and objectives for any project on which they work or propose (Figure 9.4).

Figure 9.4

Software engineers shall ensure proper and achievable goals and objectives for any project on which they work or propose (clause 3.02).

3.03 Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

3.04 Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.

3.05 Ensure an appropriate method is used for any project on which they work or propose to work.

3.06 Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.

3.07 Strive to fully understand the specifications for software on which they work.

3.08 Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.

3.09 Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.

3.10 Ensure adequate testing, debugging, and review of software and related documents on which they work.

3.11 Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

3.12 Work to develop software and related documents that respect the privacy of those who will be affected by that software.

3.13 Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.

3.14 Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

3.15 Treat all forms of software maintenance with the same professionalism as new development.

Principle 4: Judgment

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

4.01 Temper all technical judgments by the need to support and maintain human values.

4.02 Only endorse documents either prepared under their supervision or within their areas of competence and

with which they are in agreement.

4.03 Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.

4.04 Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05 Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06 Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

Principle 5: Management

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance. In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of

quality and reduction of risk.

5.02 Ensure that software engineers are informed of standards before being held to them.

5.03 Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04 Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05 Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06 Attract potential software engineers only by a full and accurate description of the conditions of employment.

5.07 Offer fair and just remuneration.

5.08 Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09 Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing,

or other intellectual property to which a software engineer has contributed.

5.10 Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11 Not ask a software engineer to do anything inconsistent with this Code.

5.12 Not punish anyone for expressing ethical concerns about a project.

Principle 6: Profession

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01 Help develop an organizational environment favorable to acting ethically (Figure 9.5).

Figure 9.5

Software engineers shall help develop an organizational environment favorable to acting ethically (clause 6.01).

6.02 Promote public knowledge of software engineering.

6.03 Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04 Support, as members of a profession, other software engineers striving to follow this Code.

6.05 Not promote their own interest at the expense of the profession, client or employer.

6.06 Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07 Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08 Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09 Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10 Avoid associations with businesses and organizations which are in conflict with this code.

6.11 Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12 Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13 Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

Principle 7: Colleagues

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01 Encourage colleagues to adhere to this Code.

7.02 Assist colleagues in professional development

7.03 Credit fully the work of others and refrain from taking undue credit.

7.04 Review the work of others in an objective, candid, and properly documented way.

7.05 Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06 Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07 Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08 In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

Principle 8: Self

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01 Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02 Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time (Figure 9.6).

Figure 9.6

Software engineers shall continually endeavor to improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time (clause 8.02).

8.03 Improve their ability to produce accurate, informative, and well-written documentation

8.04 Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05 Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06 Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07 Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08 Not influence others to undertake any action that involves a breach of this Code.

8.09 Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

9.4 Analysis of the Code

In this section we analyze the Software Engineering Code of Ethics and Professional Practice and derive an alternate set of underlying principles upon which it rests.

9.4.1 Preamble

The preamble to the code points out that there is no mechanical process for determining the correct actions to take when faced with a moral problem. Our experience evaluating moral problems related to the introduction and use of information technology confirms this statement. Even two people with similar philosophies may reach different conclusions when confronted with a moral problem. Two Kantians may agree on the basic facts of a moral problem but disagree on how to characterize the will of the moral agent. Two utilitarians may agree on the benefits and harms resulting from a proposed action but assign different weights to the outcomes, causing them to reach opposite conclusions.

The preamble also warns against taking an overly legalistic view of the code. Simply because an action is not expressly forbidden by the code does not mean it is morally acceptable. Instead, judgment is needed to detect when a moral problem has arisen and to determine the right thing to do in a particular situation.

While the code is expressed as a collection of rules, these rules are based on principles grounded in different ethical theories. This is not surprising, considering that the code was drafted by a committee. When we encounter a situation where two rules conflict, the preamble urges us to ask questions that will help us consider the principles underlying the rules. These questions demonstrate the multifaceted grounding of the code:

1. *Who is affected?*

   Utilitarians focus on determining how an action benefits or harms other people.

2. *Am I treating other human beings with respect?*

   Kant's Categorical Imperative (Section 2.6.1) tells us to treat others as ends in themselves rather than simply as a means to an end.

3. *Would my decision hold up to public scrutiny?*

   In other words, does the action reflect well on my character? Developing a good character is central to virtue ethics.

4. *How will those who are least empowered be affected?*

   Rawls's second principle of justice (Section 2.9.2) requires us to consider whether inequalities are to the greatest benefit of the least advantaged members of society.

5. *Are my acts worthy of the ideal professional?*

   Virtue ethics is based on imitation of morally superior role models.

9.4.2 Alternative List of Fundamental Principles

The start of each section of the code begins with the statement of a fundamental principle. For example, the first section begins with the fundamental principle, "Software engineers shall act consistently with the public interest." All these statements of fundamental principles are expressed

from the point of view of what software engineers ought to do.

Another way to devise a list of fundamental principles is to consider those virtues we would like to instill among all the members of any profession. We end up with a set of general, discipline-independent rules that cut across the eight categories of the code. Here is an alternative list of fundamental principles derived using that approach.

1. *Be impartial.*

   The good of the general public is equally important as the good of your organization or company. The good of your profession and your company are equally important to your personal good. It is wrong to promote your agenda at the expense of your firm, and it is wrong to promote the interests of your firm at the expense of society. (Supports clauses 1.02, 1.03, 1.05, 1.07, 3.03, 3.12, 4.01, and 6.05.)

2. *Disclose information that others ought to know.*

   Do not let others come to harm by concealing information from them. Do not make misleading or deceptive statements. Disclose potential conflicts of interest. (Supports clauses 1.04, 1.06, 2.06, 2.07, 3.01,

4.05, 4.06, 5.05, 5.06, 6.07, 6.08, 6.09, 6.12, and 6.13.)

3. *Respect the rights of others*.

   Do not infringe on the privacy rights, property rights, or intellectual property rights of others. (Supports clauses 2.02, 2.03, 2.05, and 3.13.)

4. *Treat others justly*.

   Everyone deserves fair wages and appropriate credit for work performed. Do not discriminate against others for attributes unrelated to the job they do. Do not penalize others for following the Code. (Supports clauses 5.06, 5.07, 5.08, 5.09, 5.10, 5.11, 5.12, 7.03, 7.04, 7.05, 7.07, and 8.07.)

5. *Take responsibility for your actions and inactions*.

   As a moral agent, you are responsible for the things you do, both good and bad. You may also be responsible for bad things that you allow to happen through your inaction. (Supports clauses 1.01, 3.04, 3.05, 3.06, 3.07, 3.08, 3.10, 3.11, 3.14, 3.15, 4.02, and 7.08.)

6. *Take responsibility for the actions of those you supervise*.

   Managers are responsible for setting up work assignments and training opportunities to promote quality and reduce risk. They should create effective communication channels with subordinates so that they can monitor the work being done and be aware of any quality or risk issues that arise. (Supports clauses 5.01, 5.02, 5.03, and 5.04.)

7. *Maintain your integrity*.

   Deliver on your commitments and be loyal to your employer, while obeying the law. Do not ask someone else to do something you would not be willing to do yourself. (Supports clauses 2.01, 2.04, 2.08, 2.09, 3.01, 3.02, 3.09, 4.03, 4.04, 6.06, 6.10, 6.11, 8.08, and 8.09.)

8. *Continually improve your abilities*.

   Take advantage of opportunities to improve your software engineering skills and your ability to put the Code to use. (Supports clauses 8.01, 8.02, 8.03, 8.04, 8.05, and 8.06.)

9. *Share your knowledge, expertise, and values*.

Volunteer your time and skills to worthy causes. Help bring others to your level of knowledge about software engineering and professional ethics. (Supports clauses 1.08, 6.01, 6.02, 6.03, 6.04, 7.01, 7.02, and 7.06.)

In the following section, we use these fundamental, discipline-independent principles to facilitate our analysis in four case studies related to computing.

9.5 Case Studies

Throughout this text we have evaluated a wide range of moral problems. Our methodology has been to evaluate the moral problem from the point of view of one or more of these theories: Kantianism, act utilitarianism, rule utilitarianism, social contract theory, and virtue ethics.

Another way to evaluate information technology–related moral problems is to make use of the Software Engineering Code of Ethics and Professional Practice. We follow a three-step process:

1. Consult the list of fundamental principles and identify those that are relevant to the moral problem.
2. Search the list of clauses accompanying each of the relevant fundamental principles to see which speak most directly to the issue.
3. Determine whether the contemplated action aligns with or contradicts the statements in the clauses. If the action is in agreement with all the clauses, that provides strong evidence the action is moral. If the action is in

disagreement with all the clauses, it is safe to say the action is immoral.

Usually, the contemplated action is supported by some clauses and opposed by others. When this happens, we must use our judgment to determine which of the clauses are most important before we can reach a conclusion about the morality of the contemplated action.

In the remainder of this section, we apply this methodology to four case studies.

9.5.1 Software Recommendation

Scenario

Robert Lone Wolf calls the Department of Computer Science at East Dakota State University seeking advice on how to improve the security of his business's local area network. An administrative assistant in the department routes Mr. Lone Wolf's call to Professor Adah Singh, an internationally

recognized expert in the field. Professor Singh answers several questions posed by Mr. Lone Wolf regarding network security. When Mr. Lone Wolf asks Professor Singh to recommend a software package to identify security problems, Professor Singh tells him that NetCheks got a personal computer magazine's top rating. She does not mention that the same magazine gave a "best buy" rating to another product with fewer features but a much lower price. She also fails to mention that NetCheks is a product of a spin-off company started by one of her former students and that she owns 10 percent of the company.

Analysis

From our list of nine fundamental principles, three are most relevant here:

- Be impartial.
- Disclose information that others ought to know.
- Share your knowledge, expertise, and values.

Searching the list of clauses identified with these fundamental principles, the following ones seem to fit the case study most closely:

- *1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.*

  Professor Singh was deceptive when she mentioned the most highly rated software package but not the one rated to be a "best buy."

- *1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.*

- *4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.*

- *6.02. Promote public knowledge of software engineering.*

  Professor Singh freely provided Robert Lone Wolf with valuable information about

network security.

- *6.05. Not promote their own interest at the expense of the profession, client or employer.*

  Professor Singh did not tell Robert Lone Wolf that she had a personal stake in the success of the NetCheks software. She did not tell him about the "best buy" package that might have provided him every feature he needed at a much lower price.

430

Mr. Lone Wolf was asking Professor Singh for free advice, and she provided it. When she freely shared her knowledge about network security, she was acting in the spirit of clauses 1.08 and 6.02, and doing a good thing.

However, Professor Singh appears to have violated the other three clauses, at least to some degree. Most important, she did not reveal her personal interest in NetCheks, which could lead her to be biased. The fact that she did not mention the "best buy" package is evidence that she was neither evenhanded nor completely forthcoming when she answered Mr. Lone Wolf's question about software packages.

Perhaps Mr. Lone Wolf should have heeded the maxim, “Free advice is worth what you pay for it.” Nevertheless, the naivete of one person does not excuse the bad behavior of another. Professor Singh should have revealed her conflict of interest. At that point Mr. Lone Wolf could have chosen to get another opinion if he so desired.

9.5.2 Child Pornography

Scenario

Van Nguyen, a system administrator for a large corporation, is installing a new software package on the PC used by employee Chuck Dennis. The company has not authorized Van to read other people’s emails, Web logs, or personal files. However, in the course of installing the software, he accidentally comes across directories containing files

with suspicious-looking names. He opens a few of the files and discovers they contain child pornography. Van believes possessing such images is against federal law. What should he do?

Analysis

Looking over the list of nine fundamental principles, we find these to be most relevant to our scenario:

- Be impartial.
- Respect the rights of others.
- Treat others justly.
- Maintain your integrity.

We examine the list of clauses associated with these four fundamental principles and identify those that are most relevant:

- *2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.*

Somebody has misused the company's PC by using it to store images of child pornography. By this principle Van has an obligation to report what he discovered.

- *2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.*

  While revealing the existence of the child pornography may harm the employee, possessing child pornography is illegal. Applying this principle would lead Van to disclose what he discovered.

- *3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.*

  Van discovered the child pornography by violating the company's policy against examining files on personal computers used by employees.

- *5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.*

  Simply because Chuck had these files on his computer does not necessarily mean he is guilty. Perhaps someone else broke into Chuck's computer and stored the images there.

Our analysis is more complicated because Van violated company policy to uncover the child pornography on Chuck's PC. Once he has this knowledge, however, the remaining principles guide Van to reveal what he has discovered to the relevant authorities within the corporation, even though management may punish Van for breaking the privacy policy. There is the possibility that Chuck is a victim. Someone else may be trying to frame Chuck or use his computer as a safe stash for their collection of images. Van should be discreet until a complete investigation is completed and Chuck has had the opportunity to defend himself.

9.5.3 Antiworm

Scenario

The Internet is plagued by a new worm that infects PCs by exploiting a security hole in a popular operating system. Jamila Jackson creates an antiworm that exploits the same security hole to spread from PC to PC. When Jamila's antiworm gets into a PC, it automatically downloads a software patch that plugs the security hole. In other words, it fixes the PC so that it is no longer vulnerable to attacks via that security hole [5].

Jamila releases the antiworm, taking precautions to ensure that it cannot be traced back to her. The antiworm quickly spreads throughout the Internet, consuming large amounts of network bandwidth and entering millions of computers. To system administrators, it looks just like another worm, and they battle its spread the same way they fight all other worms [6].

Analysis

These fundamental principles are most relevant to the antiworm scenario:

- Continually improve your abilities.
- Share your knowledge, expertise, and values.
- Respect the rights of others.
- Take responsibility for your actions and inactions.

Examining the list of clauses associated with each of these fundamental principles reveals those that are most relevant to our case study:

- *1.01. Accept full responsibility for their own work*.

  Jamila tried to prevent others from discovering that she was the author of the antiworm. She did not accept responsibility for what she had done.

- *1.08. Be encouraged to volunteer professional skills to good causes and contribute to public*

education concerning the discipline.

The antiworm did something good by patching security holes in PCs. Jamila provided the antiworm to the Internet community without charge. However, system administrators spent a lot of time trying to halt the spread of the antiworm, a harmful effect.

- *2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent*.

  Jamila's "client" is the community of Internet PC owners who happen to use the operating system with the security hole. While her antiworm was designed to benefit them, it entered their systems without their knowledge or consent. The antiworm also consumed a great deal of network bandwidth without the consent of the relevant telecommunications companies.

- *8.01. Further their knowledge of developments in the analysis, specification,*

design, development, maintenance, and testing of software and related documents, together with the management of the development process.

- *8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.*
- *8.06. Improve their knowledge of this Code, its interpretations and its application to their work.*

  Jamila followed the letter of the first two of these three clauses when she acquired a copy of the worm, figured out how it worked, and created a reliable antiworm in a short period of time. The experience improved her knowledge and skills. Perhaps she should invest some time improving her ability to interpret and use the Code of Ethics!

According to some of these principles, Jamila did the right thing. According to others, Jamila was wrong to release the antiworm. How do we resolve this dilemma? We can simplify our analysis by deciding that Jamila's welfare is less important than

the public good. Using this logic, we no longer consider the fact that Jamila improved her technical knowledge and skills by developing and releasing the antiworm.

That leaves us with three clauses remaining (1.01, 1.08, and 2.03). From the point of view of clause 1.01, what Jamila did was wrong. By attempting to hide her identity, Jamila refused to accept responsibility for launching the antiworm. She has clearly violated the Code of Ethics in this regard.

When we evaluate Jamila's action from the point of view of clause 1.08, we must determine whether her efforts were directed to a "good cause." Certainly, Jamila's antiworm benefited the PCs it infected by removing a security vulnerability. However, it harmed the Internet by consuming large amounts of bandwidth, and it harmed system administrators who spent time battling it. Because there were harmful as well as beneficial consequences, we cannot say that Jamila's efforts were directed to a completely good cause.

Finally, let's evaluate Jamila's action from the point of view of clause 2.03. Even though the antiworm

was completely benevolent, Jamila violated the property rights of the PC owners, because the antiworm infected their PCs without authorization. Hence Jamila release of the antiworm was wrong from the point of view of this clause.

To summarize our analysis, Jamila's release of the antiworm is clearly wrong from the point of view of clauses 1.01 and 2.03. It is also hard to argue that she satisfied the spirit of clause 1.08. We conclude that Jamila's action violated the Software Engineering Code of Ethics and Professional Practice.

9.5.4 Consulting Opportunity

Scenario

Acme Corporation licenses a sophisticated software package to many state, county, and city governments. Government agencies have the choice of three levels of service: the bronze level provides online support only; the silver level adds phone support; and the gold level includes training classes taught on the customer's site. The gold level of support costs $20,000 a year more than the silver level.

Jean is one of the Acme employees who works in the support organization. Mostly, Jean provides phone support, but from time to time she teaches an on-site class. In fact, Jean created many of the instructional materials used in these classes. Because of an economic recession, quite a few government agencies have dropped from the gold level of support to the silver level, and some members of Jean's training group have lost their jobs. Jean has a family to support, and she is wondering if her position will soon be eliminated as well.

The state government of East Dakota is one of the many customers that no longer pays Acme Corporation for on-site training. One day Jean gets

a call from Nadia, who works for the East Dakota state agency using the software package. Nadia offers to pay Jean $5,000 plus expenses to run a five-day training class that covers the same material as the official course taught by Acme.

Jean accepts the offer, but she does not inform anyone at Acme Corporation of her decision. Working at home on evenings and weekends, she develops her own set of instructional materials. She takes a week of paid vacation from work, travels to East Daktoa, and teaches the class.

Analysis

From our list of fundamental principles, quite a few are relevant here:

- Be impartial.
- Take responsibility for your actions and inactions.
- Disclose information that others ought to know.
- Maintain your integrity.

- Continually improve your abilities.
- Maintain your integrity.
- Continually improve your abilities.

Examining the clauses associated with each of these fundamental principles, the ones that most closely fit this case study are as follows:

- *2.08 Accept no outside work detrimental to the work they perform for their primary employer.*

  Employers provide employees with weekends off and paid vacations so that they can rest from their labors and return to work refreshed and able to perform at a high level. You could argue that Jean's consulting work was detrimental to her "day job" at Acme Corporation because it filled her evenings and weekends and kept her from getting a proper vacation.

- *3.04 Ensure that they are qualified for any project on which they work or propose to*

work by an appropriate combination of education and training, and experience.

Based on her prior experience at Acme, Jean was certainly well qualified to develop the instructional materials and teach the class in East Dakota. She has fulfilled this obligation of the Code.

- *4.05 Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped*.

  By accepting the consulting job with the East Dakota state government, Jean created a conflict of interest between herself and Acme Corporation. Namely, it is in Jean's interest if East Dakota does not purchase the gold level of support, but it is in Acme Corporation's interest if East Dakota does buy the gold level of support. Jean violated this clause by not disclosing her consulting job to Acme Corporation.

- *6.05 Not promote their own interest at the expense of the profession, client or employer*.

By agreeing to teach the class in East Dakota, Jean put her own interest above that of her employer. Clearly, the East Dakota state government recognized a need to have some on-site training. If Jean did not accept the consulting job, the East Dakota government might have gone back to the gold level of support from Acme.

- *8.04 Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.*

  By creating her own set of instructional materials, Jean probably developed an even better understanding of the software package and its capabilities. There is a good chance she came up with some insights about better ways to teach others how to use the software. This additional knowledge will make Jean a more valuable employee of Acme Corporation.

You could argue that Jean is actually helping Acme Corporation. Governments are dropping the gold level of support because it is simply too expensive,

but phone support and online support aren't enough. If these agencies cannot find another source of on-site training, they may stop using Acme's software altogether. By providing East Dakota with affordable on-site training, Jean was helping ensure that East Dakota would remain a customer of Acme Corporation, albeit at the silver level.

435 You could also argue that Jean's work for East Dakota improved her knowledge of the software package and her ability to teach others how to use it, making her a more effective phone support person at Acme.

However, it's unlikely upper management at Acme Corporation will be convinced by any of these arguments, particularly since Jean did not disclose the offer from East Dakota before accepting it. Jean's decision is much more likely to cause management to question her loyalty to her company and her fellow employees. If the company learns about her consulting work, Jean may well be the next person laid off.

To conclude our analysis, Jean's actions were wrong and unwise. She violated clauses 2.08, 4.05, and

6.05 of the Software Engineering Code of Ethics and Professional Practice, and she may have put her full-time job in jeopardy.

9.6 Diversity, Equity, and Inclusion

9.6.1 Introduction

You may be familiar with the proverb, "Birds of a feather flock together." The scientific term for this phenomenon is **homophily**, "the principle that contact between similar people occurs at a higher rate than among dissimilar people" [7]. In the United States, there is strong racial and ethnic homophily in marriage, school friendships, work relationships, and even appearing together in public [7].

It's more comfortable to hang out with people you see as similar. Why, then, are universities and workplaces focusing on increasing **diversity**, defined as "the representation or composition of various social identity groups in a work group, organization, or community" [8]? One reason is simple justice. No one should be excluded from pursuing an educational or professional opportunity based on their race, ethnicity, sex, sexual orientation, gender, religion, political affiliation, etc., yet underrepresentation of certain groups is

commonplace. A second reason is demographics. The United States is quickly becoming more diverse. As an illustration, non-Hispanic white people now comprise less than 35 percent of the residents of California, the most populous state. To thrive in the future, a university or company must be able to attract people from historically underrepresented groups. A third reason for promoting diversity is that it leads to better organizational performance, as the following studies demonstrate.

In an experiment at the University of Illinois, three-person teams of students were tasked with solving a murder mystery. Every team member was given a packet of information containing clues. Most clues were contained in every team member's materials, but each team member also had four important clues possessed by no other team member. To solve the mystery, the team members had to effectively share their unique clues. Groups were either men-only or women-only. Some groups had three white members. Other groups had two white members and one Black member. The racially diverse teams significantly outperformed the teams made up of only white members. The authors concluded that "surface-level diversity triggers expectations that informational differences may be present in groups, making it more expected and legitimate for group members to raise and

discuss unique information that may be critical for group performance" [9].

Another experiment with students focused on political differences. Each student participant, after revealing their political affiliation, was asked to solve a problem, then told to prepare for a meeting with another student who had come up with a different solution to the problem. The researchers observed that, on average, people who expected to meet with someone from the same political party were more focused on maintaining a relationship with that person and less focused on thoughtfully completing the task, compared with people who expected to meet with someone from a different political party. The researchers concluded that when there are disagreements to be hashed out, socially heterogeneous teams make better decisions [10].

In short, we may not be as comfortable when we are in a diverse group, but that's a good thing. When we are around people different from ourselves, we work harder, take less for granted about our teammates, and produce better results. It should be no surprise, then, that there is a strong positive correlation between higher levels of diversity in companies and greater profitability [11].

However, diversity alone isn't sufficient for organizational transformation. For people from historically underrepresented groups to fully contribute to an organization's mission, equity and inclusion are needed as well. According to the American Psychological Association:

- "**Equity** involves providing resources according to the need to help diverse populations achieve their highest state of health and other functioning" [8]. The concept of equity addresses imbalanced social systems that have disadvantaged certain groups by providing these groups with additional resources to help them achieve their full potential.

- "**Inclusion** strives for an environment that offers affirmation, celebration, and appreciation of different approaches, styles, perspectives, and experiences" [8]. The concept of inclusion recognizes that it is not enough for underrepresented people to be present; their perspectives and experiences must be welcomed.

In this section we look at some challenges facing the computing community and steps that can be taken to improve its diversity, equity, and inclusion.

9.6.2 Gender Bias in Computing

The percentage of women in computing roles in the United States has declined in the past 25 years, and the situation is particularly acute for women of color [**11**]. Women comprise only a quarter of students taking the AP computer science exam in high school, a fifth of students graduating with bachelor's degrees in computer science, and a quarter of the computing workforce [**11**]. Less than five percent of the bachelor's degrees in computer and information sciences are awarded to Black, Latina, or Indigenous women [**11**]. Less than two percent of the computer science faculty at US universities are Black, Latina, or Indigenous women [**12**].

When a profession is dominated by men, unconscious gender bias can affect important design decisions. For example, in the United States the leading cause of fetal death due to maternal trauma is automobile accidents. Seatbelts don't protect pregnant women and their unborn children properly. When crash test dummies are designed to model the average adult male, pregnant women (as well as men significantly larger or smaller than the average adult male) may suffer harm [**13**]. Another example is the HealthKit app. Apple

claimed the app would "monitor all of your metrics that you're most interested in," but the original app did not allow women to track their menstrual cycle [**14**].

Research shows that women and men tend to have different approaches to writing and debugging software, and they use programming tools differently [**15**]. Many products are designed with the intention of being gender-neutral: appealing to both women and men. If everyone on the team is a man, what may they unconsciously overlook?

Even if there are some women on the team, they may not feel free to express themselves. Some companies have a culture that encourages team members to brainstorm ideas and vote on which ones to implement. Voting tends to suppress minority views. Many women are reluctant to waste political capital by proposing or speaking up for ideas that they believe will just get voted down anyway. Many decisions related to the final product are made informally and under time pressure. If nearly all the developers are men, the perspective of the women may not be heard [**16**].

One way to address the problem of gender bias in software product development is to increase the percentage of women actively engaged in the process. What can be done to increase the number of women in software development and

leadership positions? Job postings are a practical place to start. In the United States, Title VII of the Civil Rights Act of 1964 made it illegal for job advertisements to indicate gender preferences. However, there is evidence that people creating job advertisements in fields dominated by men continue to convey, either subtly or unconsciously, the gender of the ideal candidate. Women are less likely to apply for a position when the advertisement contains a lot of masculine-themed words, such as active, adventurous, aggressive, ambitious, analytical, assertive, challenging, competitive, decisive, independent, leader, outspoken, and self-reliant. Interestingly, men are just as likely to apply for a position when the advertisement contains a lot of feminine-themed words, such as committed, compassionate, connected, cooperative, dependable, empathetic, honest, interpersonal, kind, loyal, polite, responsible, and trusting [**17**].

Simply drawing women into software organizations will not solve the problem unless the culture of these organizations also changes. More than half of women who enter the tech field drop out by midcareer, "driven out by hostile work environments and extreme job pressures" [**18**]. Women feel isolated and lack mentors. They encounter macho cultures. Two-thirds of them experience sexual harassment [**18**]. Lauren Weinstein, a man with more than 40 years'

experience in the tech industry, says, “We see these stories, ‘Why aren't there more women in computer science and engineering?’ and there’s all these complicated answers like, ‘School advisers don’t have them take math and physics,’ and it’s probably true. But I think there’s probably a simpler reason, which is these guys are just jerks, and women know it” [**19**].

9.6.3 Inclusive Language and Behavior

It’s important to reflect on how the words we use are heard by those around us. Many people unintentionally use words or phrases that perpetuate stereotypes or offend certain members of the community. By using more inclusive language, we help ensure that everyone in the community feels respected.

Here are some suggestions for making your language more inclusive:

- Refer to individuals using the pronouns they use to refer to themselves: “she/her,” “he/him,” “they/them,” or something else.

- Pay attention to the words people use to describe themselves and call them by those words. Understand that these words may change over time.
- Use person-first language rather than identity-first language. For example, instead of saying “homeless person,” you can say “person without housing.” In this way, you show respect for the value of the individual as a person. However, some communities, such as the deaf community, prefer to put the descriptor first, and in that case the community’s preference should be respected, as discussed in the previous point.
- Use gender-neutral language when referring to an unknown person. Rather than referring to a hypothetical person as “he” or “s/he,” it’s better to use “they,” as in “When a student graduates, they receive a diploma.”
- Find alternatives to words that reinforce stereotypes. To give two examples, you can replace “chairman” with “chair” or “chairperson,” and you can replace “mothering” with “caring” or another suitable word.
- Do not use derogatory terms related to mental health conditions, such as “crazy,” “mad,” or “psycho.”

It is also important to avoid the use of offensive or exclusionary language. The Diversity and Inclusion Council of the Association for Computing Machinery has identified words and phrases that it suggests should be avoided in publications and presentations, along with acceptable alternatives (see Table 9.1).

Table 9.1

Charged computing terminology and suggested alternatives [**20**].

Computing Term(s)	Issue	Alternative Term(s)
abort, terminate	violent imagery	cancel, force quit, stop, end, finalize
average user	pejorative to less experienced users	common, standard, or typical user
black/white box	racially charged	opaque/clear box
blackhat/whitehat	racially charged	unethical attacker/ethical attacker, hostile force/friendly force
blacklist/whitelist	racially charged	blocklist/allowlist, unapprovedlist/approvedlist

Computing Term(s)	Issue	Alternative Term(s)
blind, blind review	offensive to people who are blind or visually impaired	anonymous, anonymous review
byzantine	denigrating cultural stereotype	faulty, corrupted, malicious, deviant, deceptive, demonic, perfidious, inconsistent, unreliable
dark pattern	implies “dark” means bad or deceptive	deceptive pattern, manipulative pattern
daughter board	sexist	auxiliary board, ancillary board, secondary board
dummy head	derogatory term	temp head, temporary head, mock head
female/male connectors	sexist and normative terms	socket/plug connectors
gender bender		plug/socket adapter
master/slave	racially charged	primary/secondary, primary/replica, main/secondary, leader/follower, parent/child,

Computing Term(s)	Issue	Alternative Term(s)
		coordinator/worker, host/client
orphaned object		unreferenced object, dereferenced object, unlinked object
quantum supremacy	term “supremacy” is “associated	quantum advantage

Inclusive behaviors are the things we do to affirm those around us and make them feel valued and appreciated. Using inclusive language is an important component of inclusive behavior, but there are other things you can do to signal to others that you welcome their presence and appreciate what they have to say [**21**, **22**]. In particular:

- Acknowledge people when they enter the room.
- Carefully listen to how they pronounce their name and focus on pronouncing it correctly.
- Practice active listening, which means focusing on what they are saying and providing non-verbal and verbal feedback until they feel understood.

- Identify and deal with your emotional triggers. Remember that if someone pushes your buttons, that says more about you than it does about them. After all, they are *your* buttons.
- Understand and appreciate the contribution that each person can make.
- Ensure that everyone's voice is heard.

)

9.6.4 Best Practices

A symposium of experts produced a list of best practices that organizations can take to advance their diversity, equity, and inclusion efforts [**23**]:

- Establish numerical goals for diversity and track progress toward achieving these goals by regularly collecting and analyzing data, identifying obstacles, and planning strategies to continue making progress.
- Create alternative pathways for employees to lodge discrimination and harassment complaints. About half of workers who file discrimination or harassment complaints suffer retaliation. Companies can make it safer for employees to lodge complaints by setting up ombuds offices or allowing employee assistance plans run by outside vendors to handle the complaints.

- Before deploying technologies for screening, hiring, and evaluating employees, audit them to ensure they do not have racial, ethnic, or gender biases.
- Avoid small-N problems. When an organization has a small number of people from an underrepresented group, they may suffer from tokenism or be judged according to stereotypes. A way to counter this is to increase the visibility of underrepresented groups by bringing members of these groups into the organization to make presentations. Another small-N problem arises when companies fill positions one at a time. Instead of hiring a new software engineer every quarter, a growing company could hire four new software engineers every summer. This strategy has been shown to result in less bias.
- Rather than engaging an expert to design a diversity program that is then given to managers to execute, an organization should involve its managers in the design of the program. In this way, the company can increase the buy-in of its managers and help ensure the program's success.

Salesforce is an example of a large tech company that has demonstrated significant progress toward achieving diversity, equality, and inclusion. The effort began in 2015 when Salesforce conducted a salary audit and spent $3 million to eliminate the company's gender pay gap [**24**]. The next step was the creation of the High-Potential Leadership Program, which focused on providing women with leadership training. The result was a 33 percent increase in the annual number of women who were promoted [**24**]. After the murder of George Floyd in 2020, Salesforce created a Racial Equality and Justice Task Force. By following the best practices described above, the company grew the number of employees from under-represented groups and doubled the number of Black employees in leadership positions (defined as vice president or above) [**25**]. Salesforce has collected data to track its progress diversifying its workforce, and it has shared the results on a Web site (www.salesforce.com/company/equality).

9.7 Whistle-Blowing

All four case studies presented in Section 9.5 involve the actions of a single individual. It is easy for us to assign moral responsibility to that person and to discuss how things might have turned out better if they had acted differently. Often, however, a product or decision is the cumulative result of the work of many people within a larger organization. Suppose somebody within the organization perceives a danger to the public but is unable to persuade the rest of the organization to make needed changes to eliminate that danger. Should that person go outside the organization with the information?

A **whistle-blower** is someone who breaks ranks with an organization in order to make an unauthorized disclosure of information about a harmful situation after attempts to report the concerns through authorized organizational channels have been ignored or rebuffed [26]. Sometimes employees become whistle-blowers out of fear that actions taken by their employer may harm the public; other times they have identified fraudulent use of tax dollars [27].

9.7.1 Morton Thiokol/NASA

On January 28, 1986, the space shuttle *Challenger* lifted off from Cape Canaveral. On board were seven astronauts, including schoolteacher Christa McAuliffe, the first civilian to fly into space. Just 73 seconds after liftoff, hot gases leaking from one of the booster rockets led to an explosion that destroyed the *Challenger* and killed everyone on board (Figure 9.7).

Figure 9.7

The explosion of the *Challenger* killed seven astronauts, including the first civilian in space, Christa McAuliffe.

(Courtesy of NASA)

Engineer Roger Boisjoly was in charge of inspecting the O-rings on the boosters recovered after launches of the space shuttle. The O-rings were supposed to seal connections between sections of the booster rockets. On two occasions in

1985, he had seen evidence that a primary O-ring seal had failed. Boisjoly presented a report on his findings to NASA officials at the Marshall Space Flight Center. Frustrated that NASA officials were not giving sufficient attention to the problem, he wrote a memo to vice president for engineering Robert Lund, stating that an O-ring failure could lead to the loss of a shuttle flight and the launch pad. Despite Boisjoly's persistent efforts to get the seals redesigned, the problem was not fixed.

On January 27, 1986, Boisjoly and a group of Morton Thiokol engineers met to discuss the proposed launch for the following day. Florida was in the middle of an unusual cold snap; the weather forecast for northern Florida called for an overnight low of 18 degrees Fahrenheit. The engineers knew that frigid temperatures greatly increased the probability that an O-ring would fail, allowing hot gases to escape from a booster rocket. They prepared a set of 14 slides that documented their concern about a low-temperature launch.

The evening of January 27, Morton Thiokol had a teleconference with the Marshall Space Flight Center and the Kennedy Space Center. Morton Thiokol's presentation ended with the engineers' recommendation that NASA not launch the *Challenger* if the temperature was below 53 degrees.

NASA asked Morton Thiokol vice president Joe Kilminster for a go/no-go decision. Kilminster said his recommendation was not to launch.

NASA officials were displeased to get this recommendation from Morton Thiokol. The launch had already been delayed several times. They were eager to launch the space shuttle before the president's State of the Union address the following evening, so that the president could include the mission in his speech. After NASA officials expressed their dismay with the recommendation, Kilminster asked for a five-minute break in the proceedings.

During the recess, Morton Thiokol's four top managers huddled away from the engineers. Senior vice president Jerald Mason and vice president Calvin Wiggins supported the launch, while vice presidents Joseph Kilminster and Robert Lund were opposed. However, Lund changed his mind after Mason "told him to take off his engineering hat and put on his management hat" [28]. (More than half of Morton Thiokol's profits came from its work for NASA.)

When Morton Thiokol rejoined the teleconference, Kilminster told NASA officials that Morton Thiokol recommended the launch go ahead. NASA officials at the Marshall Space Flight Center prevented the engineers'

negative recommendation from being communicated to the NASA officials with final authority to approve or delay the launch.

A month after the loss of the *Challenger*, Boisjoly testified before a presidential commission appointed to investigate the disaster. Morton Thiokol lawyers had advised Boisjoly to reply to every question with a simple yes or no. Instead, Boisjoly shared with the commission his hypothesis about how the cold temperature had caused the failure of an O-ring. In later meetings with commission members, he presented documents that supported his hypothesis, including his 1985 memo. Boisjoly's testimony and documents contradicted the testimony of Morton Thiokol management. The company responded by isolating Boisjoly from NASA personnel and the O-ring redesign effort [**28**, **29**].

Distressed by the hostile environment, Boisjoly stopped working for Morton Thiokol in July 1986. Two years later, he found work as a forensic engineer.

9.7.2 Hughes Aircraft

In the 1980s, Hughes Aircraft manufactured military-grade hybrid computer chips at its Microelectronic Circuit Division in Newport Beach, California. (A hybrid computer chip

contains both digital and analog circuits.) The division produced about 100,000 hybrid chips per year. The military put these chips in a variety of sophisticated weapons systems, such as fighter planes and air-to-air missiles. Manufacturing these chips was a lucrative business for Hughes Aircraft: the government paid between $300 and $5,000 for each chip.

In return for paying these high prices, the government insisted that the chips pass stringent quality-assurance tests. Hughes Aircraft technicians made two kinds of tests. First, they ensured the chips functioned correctly. Second, they checked the chips for resistance to shocks, high temperatures, and moisture. About 10 percent of the chips failed at least one of these tests. A common problem was that a chip would have a defective seal, which let moisture in. These chips were called “leakers.”

Margaret Goodearl and Donald LaRue supervised the testing area. The company hired Ruth Ibarra to be an independent quality-control agent.

In August 1986, floor worker Lisa Lightner found a leaker. Donald LaRue ordered her to pass the chip. Lightner told Goodearl, and Goodearl reported the incident to upper management. Hughes Aircraft management threatened to fire

Goodearl if she didn't reveal the identity of the worker who had complained.

Two months later LaRue ordered Shirley Reddick, another floor worker, to reseal lids on some hybrid chips, in violation of the required process for handling leakers. Reddick reported the incident to Goodearl, who relayed the report to upper management. Again, Goodearl was told she might be fired if she kept up this pattern of behavior.

In the same month, LaRue asked tester Rachel Janesch to certify that a defective hybrid chip had passed the leak test. Goodearl played a role in reporting the incident to Hughes Aircraft management. In this case the chips were retested.

Goodearl and Ibarra found a box of hybrid chips with blank paperwork, meaning the necessary tests had not been performed. When Goodearl reported this discovery to her superiors, they told her she was no longer part of the team. Goodearl filed a formal harassment complaint. A midlevel manager in personnel called her into his office, tore up her complaint, threw his glasses at her, and said, "If you ever do anything like that again, I will fire your ass" [27].

Goodearl's performance evaluations, which had been excellent, dropped sharply as soon as she began complaining

about irregularities in the chip testing facility. In late 1986, Goodearl and Ibarra contacted the Office of the Inspector General, part of the US Department of Justice. A joint decision was made for Goodearl and Ibarra to find a clear-cut case of fraud.

One day LaRue put two leaky hybrid chips on his desk, planning to approve them after Goodearl had gone home. Goodearl and Ibarra made photocopies of the documentation showing the chips had failed the leak test. After the chips were shipped from Hughes Aircraft, the Department of Defense tested them and found them to be leakers. As a result of this incident, the Office of the Inspector General began a formal investigation of fraud at Hughes Aircraft.

Hughes Aircraft fired Goodearl in 1989. Ibarra had left Hughes Aircraft in 1988 “after being relieved of all meaningful responsibilities and put in a cubicle with nothing to do” [30]. In 1990 Margaret Goodearl and Ruth Ibarra (now known by her married name, Ruth Aldred) filed a civil suit against Hughes Aircraft, claiming that Hughes Aircraft had violated the False Claims Act by falsifying records in order to defraud the government. This civil suit was put on hold until the end of the criminal trial.

The inspector general's criminal investigation led to a trial in 1992. The jury found Hughes Aircraft guilty of conspiring to defraud the government. Hughes Aircraft appealed the verdict, but the verdict was upheld. Since a criminal conviction can be used as evidence in a civil trial, the verdict nearly assured that Goodearl and Aldred would prevail in their civil suit. Hughes Aircraft began negotiating a settlement in the civil suit.

Four years later, Hughes Aircraft was ordered to pay $4.05 million in damages. Goodearl and Aldred received 22 percent of the settlement, or $891,000. In addition, Hughes Aircraft was required to pay their legal fees, which amounted to $450,000 [**27**, **31**].

Goodearl and Aldred paid a high price for whistle-blowing. Both were unemployed for an extended period of time. Aldred and her husband received public assistance until they could find work. Goodearl and her husband had to file for bankruptcy, and they eventually divorced. Despite these hardships, both whistle-blowers said they "would do it all again" [**32**].

9.7.3 US Legislation Related to Whistle-Blowing

Whistle- blowers are usually punished for disclosing information that organizations have tried to keep under wraps. If they do not lose their jobs outright, they have probably lost all chances for future advancement within the organization. Whistle-blowers and their families typically suffer emotional distress and economic hardship.

Nevertheless, whistle-blowers often serve the public good. For this reason the US government has passed two pieces of legislation to encourage whistle-blowing: the False Claims Act and the Whistle-blower Protection Act of 1989.

The False Claims Act was first enacted by Congress in 1863 in response to massive fraud perpetrated by companies providing supplies to the Union Army during the Civil War. The law allowed a whistle-blower to sue, on behalf of the government, a person or company that was submitting falsified claims to the government. If the organization was found guilty and forced to pay a settlement to the government, the whistle-blower received half the settlement.

In 1943 Congress amended the False Claims Act, drastically reducing the share of the settlement a whistle-blower would receive and limiting the evidence or information a whistle-blower could use in the lawsuit. As a result, the law fell into disuse.

In the mid-1980s, the media carried numerous stories about defense contractors perpetrating fraud against the government. Congress responded by amending the False Claims Act once again, making it easier for people to put together a successful lawsuit and allowing whistle-blowers to receive between 15 and 30 percent of settlements. The False Claims Act also provides certain protections to whistle-blowers against retaliation by their employers.

The Whistle-blower Protection Act of 1989 establishes certain safeguards for federal employees and former employees who claim negative personnel actions have been taken against them for whistle-blowing. Whistle-blowers can appeal to the US Merit Systems Protection Board.

9.7.4 Morality of Whistle-Blowing

Are whistle-blowers heroes or traitors? Marcia Miceli and Janet Near point out that people become whistle-blowers for different reasons. They suggest we ought to consider their motives before we decide if they were acting morally [33]. While it is fair to say that all whistle-blowers are trying to bring an end to wrongdoing, they may well have other reasons for publicizing a problem. We can evaluate the morality of whistle-blowing by considering whether the whistle-blower is motivated by a desire to help others or harm others.

Consider a person who has known about a dangerous product for years but only becomes a whistle-blower after they have been turned down for a raise or promotion. If the disgruntled employee blows the whistle in order to exact revenge on an organization that has let them down, the primary motivation is to hurt the company, not to help the public. Another example of questionable whistle-blowing is the case of employees who have been involved in a cover-up for some period of time, realize that they are about to be caught, and then cooperate with the authorities to identify other guilty parties in order to avoid punishment.

But suppose a person doesn't have ulterior motives for whistle-blowing and is doing it simply to inform the public of

a dangerous situation or a misappropriation of funds. There are three general reactions to altruistic whistle-blowing [**29**].

Whistle-Blowers Cause Harm

The typical corporate response to whistle-blowing is to condemn it. Whistle-blowers are disloyal to their companies. Through their actions they generate bad publicity, disrupt the social fabric of an organization, and make it more difficult for everyone to work as part of a team. In other words, their betrayal causes short-term and long-term damage to the company. While it is the responsibility of engineers to point out technical problems, the management of a company is ultimately responsible for the decisions being made, both good and bad. If management makes a mistake, the public has recourse through the legal system to seek damages from the company, and the board of directors or CEO can replace the managers who have used bad judgment.

The weakness in this response is its cavalier and overly legalistic attitude toward public harm. If people are hurt or killed, they or their heirs can always sue for damages. Yet surely society is better off if people are not harmed in the first place. A monetary settlement is a poor replacement for a human life.

Whistle-Blowing Is a Sign of Organizational Failure

A second response to whistle-blowing is to view it as a symptom of an organizational failure that results in harm all around [34]. The company suffers from bad publicity. The careers of accused managers can be ruined. It makes people suspicious of one another, eroding team spirit. Whistle-blowers typically suffer retaliation and become estranged from their coworkers. Labeled as troublemakers, their long-term prospects with the company are dim.

Since whistle-blowing is a sign of failure, organizations need to find a way to prevent it from happening in the first place. Some suggest that organizations can eliminate the need for whistle-blowing by creating management structures and communication processes that allow concerns to be raised, discussed, and resolved.

This may be easier said than done. Robert Spitzer observes that organizations have shifted away from principle-based decision-making to utilitarian decision making. A characteristic of rule-oriented ethical decision making is its absolute nature. According to Kantianism or social contract theory, the end never justifies the means. If an action violates

a moral rule, it shouldn't be done, period. In contrast, a utilitarian process weighs expected benefits and harms. Once an organization begins using utilitarian thinking, the question is no longer "Should we do it?" but "How much of it can we do without harm?" Spitzer writes, "One can see situations in which it would be permissible to use an evil means to achieve a good so long as enough benefit can be actualized." He suggests that organizations should return to using principle-based ethics in their decision making [35].

Whistle-Blowing as a Moral Duty

A third response is to assert that under certain circumstances people have a moral duty to blow the whistle. Whistle-blowing is alluded to in clauses 1.02, 1.03, 1.04, 1.05, 2.05, 2.09, 3.01, 6.06, and 6.13 of the Software Engineering Code of Ethics and Professional Practice. These clauses provide a justification for whistle-blowing in a variety of circumstances.

Richard De George believes whistle-blowers should ask themselves five questions:

1. Do you believe the problem may result in "serious and considerable harm to the public"?
2. Have you told your manager your concerns about the potential harm?

3. Have you tried every possible channel within the organization to resolve the problem?
4. Have you documented evidence that would persuade a neutral outsider that your view is correct?
5. Are you reasonably sure that if you do bring this matter to public attention, something can be done to prevent the anticipated harm?

According to De George, you have a right to whistle-blow if you answer yes to the first three questions; if you answer yes to all five questions, you have a duty to whistle-blow [**36**].

De George's five requirements are controversial. Some would say whistle-blowing is justified even when fewer requirements are met. For example, what if the potential whistle-blower knows about a problem that could result in death or injury to millions of people, such as a meltdown inside a nuclear power plant? The whistle-blower has communicated his concerns to their manager, but there is not time to lobby every potential decision maker in the company. They are reasonably sure that if they contacted a television station, something could be done to prevent the meltdown. At the very least, the media could alert people so that they could get out of harm's way. Shouldn't that person be obliged to

whistle-blow, even though the answer to the third question is no?

To others, insisting that the whistle-blower have convincing documentation is too strict a condition to be met in order for whistle-blowing to be a moral imperative. After all, once the whistle-blower has revealed the wrong to another organization, that organization may be in a better position to gather supporting evidence than the whistle-blower [37].

Along the same lines, some argue that whistle-blowing should be considered an obligation even when only the first three requirements are met. They hold that people should be willing to sacrifice their good and the good of their families for the greater good of society.

Others believe De George goes too far when he gives conditions under which people are morally *required* to whistle-blow. These commentators suggest that a person's obligation to whistle-blow must be weighed against that person's other obligations, such as the duty to take care of one's family. Whistle-blowing often results in significant emotional stress and the loss of employment. If it results in a person being labeled a troublemaker, whistle-blowing can end a career. Hence there are serious emotional and financial

consequences to whistle-blowing that affect not only whistle-blowers but also their spouses and children [29].

Put another way, is it reasonable to take a strictly utilitarian approach to whistle-blowing? Should we expect potential whistle-blowers to weigh the benefits to a large number of people against the harm to themselves and their families, and decide to go public? After all, the whistle-blower has already gone out on a limb to inform management of the dangerous situation. It is the managers who made the immoral decision to cover up the problem, not the whistle-blower. We are asking a lot when we ask innocent people to sacrifice their careers and the welfare of their families for the benefit of strangers. We shouldn't be surprised to learn that when whistle-blower Al Ripskis was asked what advice he would give potential whistle-blowers, his immediate reply was "Forget it!" [38, p. 34].

On the other hand, whistle-blower Carlos G. Bell Jr. chastises fellow engineers for the way they duck responsibility:

> **We engineers are almost without exception only too willing to assign moral responsibility to any administrator or executive or politician under whom we can place ourselves. Our reward for living in such ways is a part of the American dream: we are**

> **involved in very few arguments and year-by-year, we build up sizable pensions for our old age. [39]**

Moral responsibility is different from other kinds of responsibility. First of all, moral responsibility must be borne by people. While the Fourteenth Amendment to the US Constitution may make a corporation a person in the legal sense of the word, a corporation is not a moral agent. We cannot assign moral responsibility to a corporation or any other organization [40].

Second, moral responsibility is different from role responsibility, causal responsibility, and legal responsibility in that it is not exclusive [40]. **Role responsibility** is responsibility borne because of a person's assigned duties. A company may hire a bookkeeper to send out invoices and pay the bills. It is the bookkeeper's responsibility to get the bills paid on time. **Causal responsibility** is responsibility assigned to people because they did something (or failed to do something) that caused something to happen. "Joe is responsible for the network being down, because he released the virus that caused the computers to crash." **Legal responsibility** is responsibility assigned by law. Homeowners are responsible for the medical bills of a postal carrier who

slips and falls on their driveway. Role responsibility, causal responsibility, and legal responsibility can be exclusive. For example, if one person is responsible for paying the bills, the other employees are not. Moral responsibility is not exclusive. For example, when an infant is brought into a home, all the caregivers are responsible for the baby's well-being.

Because moral responsibility is not exclusive, people cannot pass the buck by saying, "My boss made the final decision, not me," or by saying, "I just wrote the software; I wasn't responsible for testing it." When people abdicate their moral responsibility, great harms can be done. For example, in the 1970s, executives at Ford Motor Company were anxious to begin selling a 2,000-pound, $2,000 alternative to Japanese imports. Unfortunately, prototypes of the Ford Pinto could not pass the mandatory collision test because the windshield kept popping out. Forbidden from making design changes that would increase the weight of the car or delay its introduction, engineers solved the problem by redirecting the energy of the collision down the drive train. They knew this change would make the gas tank more likely to rupture, but the car did not have to pass a fuel tank integrity test. Covering up design problems allowed Ford to get its subcompact car to market. However, Ford eventually paid

millions of dollars to settle dozens of lawsuits resulting from fiery crashes involving Pintos. Moreover, unfavorable media attention harmed Ford's reputation for years [38].

Michael McFarland argues that a team of engineers should be held to a higher level of moral responsibility than any of its individual members. There may well be situations where a person has a duty to speak the truth. To this duty, McFarland adds another duty held by moral agents: the duty to help others in need. If whistle-blowing should be done and no individual has the strength to do it, then it must be done by the group acting collectively [41].

Summary

A computer-related job, such as system administration, computer programming, or software engineering, is not a full-fledged profession like medicine or law, because in most cases you do not need to be certified and licensed in order to design, implement, or maintain computer hardware or software. Nevertheless, those who work with computers can, through inadequate education, insufficient practical training, or bad choices, cause a great deal of harm to members of the public. In this respect, the responsibility of computer "professionals" can be similar to that held by members of fully developed professions. For these reasons, the two largest computing societies have worked together to develop a code of ethics to guide the actions of software engineers: those who develop or maintain software and those who teach in this field.

The Software Engineering Code of Ethics and Professional Practice is based upon eight general principles related to the following subjects: the public, client and employer, product, judgment, management, profession, colleagues, and self. Each

of these general principles contains a list of clauses related to specific areas of potential moral concern for the practicing software engineer. Good judgment is still needed, however. In many situations, there is a conflict between two or more of the relevant clauses. At these times, the decision maker must determine which of the clauses is most relevant and/or most important.

The United States is becoming more diverse, and companies are recognizing the importance of promoting diversity, equity, and inclusion in order to attract the best talent and produce the best results. Computer professionals can take practical steps to support these efforts by making their own language and behavior more inclusive.

To many, whistle-blowing is a heroic act requiring great moral courage. A whistle-blower brings to light a real or potential harm to the public, such as an abuse of taxpayers' money or a defective product, after trying and failing to get the problem resolved within the organization. Inevitably, whistle-blowers and their families suffer emotionally and economically. It may take a decade for a whistle-blower to be vindicated in court.

Different commentators have taken widely different views about whistle-blowing. Some say whistle-blowing does so

much harm to the whistle-blower and the organization that it is never the right thing to do. At the other extreme are those who argue any harm done to whistle-blowers and their families is outweighed by the benefits to society, at least when certain conditions are met. In the middle are those who argue that any decision for or against whistle-blowing must be made on a case-by-case basis.

If whistle-blowing is ever called for, it is only as a last resort. Everyone agrees that people who discover real or potential harms to the public should first attempt to get the problem fixed within the organization. It would be better if there were never a need for whistle-blowing. Organizations ought to have communication and decision-making structures that make it easier to identify and deal with financial irregularities or product defects.

The predominant American corporate mind-set does not align well with this ideal. Managers focused on maximizing "the bottom line" may well make decisions on utilitarian grounds, weighing the costs and benefits of each alternative. Utilitarian thinking allows an organization to do something that is slightly bad in order to reap a greater good. Undisclosed bad deeds are less harmful than those brought to light. Hence utilitarian thinking can create an atmosphere in

which the free communication of organizational actions is suppressed. In this environment, those who wish to report financial irregularities or product defects are ignored or silenced. The financial scandals at Enron, Tyco International, WorldCom, Adelphia Communications, FTX Trading, and other corporations that cost investors billions of dollars have prompted some ethicists to call for a return to principle-based decision-making.

Further Reading, Listening, and Viewing

Dan Gotterbarn. “Why Bother with Ethics in Computing: Addressing Harmful Paradigms?” *ACM Inroads*, p. 9, March 2010.

Rob Haythorne. “Ethics in Computing: Real Ethics and Virtual Reality.” *Production Zone*, May 28, 2011. 14:19. www.youtube.com.

Peer Ludlow. “The Banality of Systemic Evil.” *New York Times*, September 15, 2013. opinion ator.blogs.nytimes.com/2013/09/15/the-banality-of-systemic-evil.

John Markoff. “Collision in the Making between Self-Driving Cars and How the World Works.” *New York Times*, January 24, 2012.

C. Dianne Martin. “Building Character.” *ACM Inroads*, p. 11, March 2010.

Jake Pearson. “Drugstore Cowboy.” *Wired*, June 2013.

Tom Simonite. “What Really Happened When Google Ousted Timnit Gebru.” *WIRED*, June 8, 2021.

https://www.wired.com/story/google-timnit-gebru-ai-what-really-happened/

Paul Solman. “How Virtual Reality Games Can Transform Society, Prosperity.” *PBS News-Hour*, July 11, 2013. 10:27. video.pbs.org.

ComputingCases.org (Web site).

Review Questions

1. In what ways is a computer-related career, such as programming or system administration, similar to a fully developed profession such as medicine? In what ways is a computer-related career unlike a fully developed profession?
2. How prevalent is licensing for software engineers in the United States?
3. Identify as many clauses as you can in the Software Engineering Code of Ethics and Professional Practice that refer to issues related to privacy.
4. Identify as many clauses as you can in the Software Engineering Code of Ethics and Professional Practice that refer to issues related to intellectual property.
5. Identify five clauses in the Software Engineering Code of Ethics and Professional Practice that reflect a utilitarian ethical viewpoint.
6. Identify five clauses in the Software Engineering Code of Ethics and Professional Practice that reflect a

Kantian ethical viewpoint.

7. Define the terms “diversity,” “equity,” and “inclusion” in your own words.
8. What is it about diverse teams that can produce higher quality work products than teams lacking diversity?
9. What are three practical steps people can take to make their language more inclusive?
10. What are three practical steps people can take to make their behavior more inclusive?
11. What is whistle-blowing? What harms does it cause? What benefits may it provide?
12. Which clauses in the Software Engineering Code of Ethics and Professional Practice support the legitimacy of whistle-blowing? Which clauses in the code may be violated by a whistle-blower (assuming the whistle-blower is telling the truth)?

Discussion Questions

13. What steps has your campus taken to improve diversity, equity, and inclusion in its computer-related majors? What steps could be taken?

14. The *Challenger* disaster led to the deaths of seven astronauts and the loss of hundreds of millions of dollars' worth of equipment. How much moral responsibility should each of the following groups hold for this tragedy: Morton Thiokol engineers, Morton Thiokol senior management, NASA management?

15. In the criminal proceedings resulting from the government's investigation of fraud at the Microelectronic Circuit Division, the jury found Hughes Aircraft guilty, but it found supervisor Donald LaRue not guilty. The jury felt LaRue was simply following orders from management. Was the jury's decision a just one?

16. Do you agree with Michael McFarland that a team of engineers has greater moral responsibility than any individual engineer on the team?

17. You are a manager in charge of a section of 30 employees in a large corporation. This morning one of your employees—Minjee Lee—enters your office and tells you she thinks two members of your staff are having an affair. These employees are married—but not to each other. Minjee is afraid that if it is true, others in the office will inevitably find out about it, harming morale and productivity. She suggests that you discreetly monitor their emails to see if they provide evidence of an affair. If you find evidence, you can nip the problem in the bud. If there is no problem, you do not have to embarrass yourself by talking with the employees. What should you do? [**42**]

18. Two weeks ago you started a new job as system administrator for a computer lab at a small college. Wanting to make a good impression, you immediately set out to learn more about the various applications provided to the users of the lab. One of the packages, an engineering design tool, seemed way out of date. You looked through the lab's file of licensing agreements to see how much it would cost to get an

upgrade. To your horror, you discovered that the college never purchased a license for the software—it is running a bootlegged copy!

When you bring this to the attention of your boss, the college's director of information technology, he says, "The license for this software would cost us $10,000, which we don't have in our budget right now. This software is absolutely needed for our engineering students, though. Maybe we can get the license next year. For the time being, just keep the current version running."

How would you respond to your manager?

19. You are a junior in college. You sent your resume to a half-dozen companies hoping to get a summer internship. Two weeks ago XYZ Corporation contacted you and offered you a paid summer internship. One week ago you accepted their offer, agreeing to start work a week after your last final exam. Today you received a much better internship offer from ABC Corporation. What should you do?

20. You are a senior in college. You sent your resume to a half-dozen companies hoping to get a job. A month ago you interviewed at ABC Corporation and XYZ

Corporation. Two weeks ago XYZ Corporation offered you a job. One week ago you accepted their offer, agreeing to start work a month after graduation. Today you received a much better offer from ABC Corporation. What should you do?

21. You are the manager of a software development group within a large corporation. Your group would be more productive if the PCs were upgraded, but you do not have any money left in your annual equipment budget. Because of employee turnover, you do have plenty of money left in your personnel budget, but corporate rules do not allow you to spend personnel funds on equipment.

    If you overspend your equipment budget, you will receive a negative performance review. You also know that whatever money is left over in your budget at the end of the fiscal year is "swept up" by the corporation. In other words, you cannot carry over a surplus from one year to the next—your group loses the money.

    You complain about your situation to the manager of another group, who has the opposite problem. They have plenty of money left in their equipment budget, but their personnel expenses are going to exceed their labor budget unless they does something. They offer to

buy you the $50,000 of equipment you need out of their budget, if you pick up $50,000 of their personnel expenses out of your budget. If you take this action, both groups will get what they need, and neither group will exceed any of its budgets.

Discuss the morality of the proposed course of action.

22. Five years ago Bandar graduated from college and began working for Superlative Software Corporation. His most recent promotion has made him the manager of a large group of software engineers and support staff. One of Bandar's responsibilities is to submit his budget request for the next fiscal year. He's never done this before, so one day over lunch he asks Li Na, a more experienced manager, for some advice.

    Li Na: Figure out what you really need to complete the projects your group will be doing, and then add another 20 percent. High-level management always cuts everybody's budget 10 to 20 percent, so after they reduce your budget, you'll still have the money you need.

    Bandar: But the memo from the vice president said we should only ask for the amount of money we really need.

Li Na: Nobody pays attention to that.

Bandar: What if they ask me to justify my budget? It'll be pretty obvious that I've padded it.

Li Na: They never do that—they don't have the time. Even if they did, you can work the numbers to justify the extra staff you'll need to meet the tight deadlines they've set.

Bandar: You mean lie?

Li Na: Look, what are you going to do if your group doesn't get the budget it needs? You won't be able to staff up for the new projects. That means you and all your current staff are going to be super-stressed all year long trying to meet the deadlines. Spare yourself a lot of grief and do what all the other managers are doing.

What would you do if you were in Bandar's position? Why?

23. Leyana interviews a candidate for a software engineering position. She feels the person has several holes in his technical background that could hinder his job performance. The next day Leyana and five other people who have interviewed the candidate meet with

the hiring manager to discuss his strengths and weaknesses. Before Leyana speaks, everyone else voices the opinion that the candidate has great technical skills and should be hired. It seems clear to her that the hiring manager wants to offer this person a job. She wonders if she should bother voicing her reservations.

What would you do if you were in Leyana's position? Why?

24. Would you characterize Edward Snowden, the person who leaked information about US surveillance programs to the British newspaper the *Guardian*, as a whistle-blower?

25. Watch "Ethics in Computing: Real Ethics and Virtual Reality" (details in **Further Reading, Listening, and Viewing**). Discuss whether Sony should have received permission from Manchester Cathedral before featuring that site in its first-person shooter game, *Resistance: Fall of Man*.

In-Class Exercises

26. A college equips its large lecture halls with wireless networks, and it requires all of its students to purchase a laptop computer when they enroll. A computer science professor plans to streamline how quizzes are administered in their introductory programming class. Students will take the quizzes online as they sit in the classroom. A computer will grade the quizzes instantly, providing the students with immediate feedback. The computer will also provide the professor with information about how well the students did on each question, which will enable them to spend more of their lecture time focusing on those topics that the students are having the hardest time understanding. Discuss the benefits and risks associated with implementing the proposed system.

27. Company X wants to open a dating service Web site. It hires Company Y to develop the software. Company Y hires Gina as a private contractor to provide a piece of instant-messaging software for the package. Gina's contract says she is not responsible for the security of

the site. Company Y is supposed to perform that bit of programming. However, software development runs behind schedule, and Company Y implements a simplistic security scheme that allows all messages to be sent in plain text, which is clearly insecure.

Gina brings her concerns to the management of Company Y. Company Y thanks her for her concern, but indicates it still plans to deliver the software without telling Company X. Company Y reminds Gina that she has signed a confidentiality agreement that forbids her from talking about the software to anyone, including Company X.

What should Gina do?

28. You are a member of the information services team at a large corporation. The president has asked for a confidential meeting with your group to talk about ways to improve productivity. The president wants to ensure that people are not sending personal emails or surfing the Web for entertainment while they are supposed to be working. The chief information officer suggests that employees be informed that their emails and Web surfing will be monitored. In truth, the company does not have the resources to do this and does not plan to implement any monitoring. The CIO

strictly forbids anyone in the information services team from revealing this fact. Debate the morality of management making such an announcement.

29. The members of the class are the employees of a small, privately held company that produces computer games. Everyone shares in the profits of the company. The company has been making electronic versions of popular board games for established game companies. Business is steady, but profits have not been large. The marketing team says that a first-person shooter game based on the war in Ukraine would generate a huge amount of publicity for the company and could be highly profitable. Debate the morality of producing such a game.

30. The Department of Homeland Security is interested in using computers to identify suspected terrorists operating within the United States. It would like to mine databases containing information about purchases and travel to detect patterns that may identify individuals who are engaged in, or at least planning, terrorist activity. It asks a panel of computer scientists to determine the feasibility of this project. A panel member says the most difficult problem will be determining what patterns of transactions to look for.

He suggests it might be possible to construct a computer program that uses artificial intelligence to mimic a terrorist organization. The program would determine the actions needed to execute a terrorist act. Once these actions were determined, it would be possible to search database records to find evidence of these actions.

Divide the class into groups of four or five students to debate the morality of developing a computer program capable of planning the steps needed to execute an act of terror.

References

[1] Edwin Black. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. Dialog Press, Washington, DC, 2011.

[2] Gary Ford and Norman E. Gibbs. "A Mature Profession of Software Engineering." Technical report, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-96-TR-004, ESC-TR-96-004, January 1996.

[3] "NCEES Discontinuing PE Software Engineering Exam." NCEES (Web site), March 13, 2018. ncees.org/ncees-discontinuing-pe-software-engineering-exam/.

[4] Gotterbarn, Don; Miller, Keith; Rogerson, Simon (1997). Software engineering code of ethics. Communications of the ACM, 40(11), 110–118. Used with permission from ACM.

[5] J. Eric Smith. "Anti-Worm Worm Makes Rounds, Cleanses Systems of Infection." *Geek.com* (blog), August 20, 2003. www.geek.com.

[6] Florence Olsen. “Attacks Threaten Computer Networks as Students Arrive for the Fall Semester.” *Chronicle of Higher Education*, September 5, 2003.

[7] Miller McPherson, Lynn Smith-Lovin, and James M. Cook. “Birds of a Feather: Homophily in Social Networks.” *Annual Review of Sociology,* 21: 415–444, January 2001.

[8] “Equity, diversity, and inclusion.” (Web page) American Psychological Association. Accessed June 26, 2023. https://www.apa.org/topics/equity-diversity-inclusion.

[9] Katherine W. Phillips, Gregory B. Northcraft, and Margaret A. Neale. “Surface-Level Diversity and Decision-Making in Groups: When Does Deep-Level Similarity Help?” *Group Processes & Intergroup Relations,* 9(4): 467–482, 2006.

[10] Denise Lewin Loyd, Cynthia S. Wang, Katherine W. Phillips, and Robert B. Lount, Jr. “Social Category Diversity Promotes Premeeting Elaboration: The Role of Relationship Focus.” *Organization Science,* 24(3): 757–772, May–June 2013. https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfile

[11] Michael Conway, Kweilin Ellingrud, Tracy Nowski, and Renee Wittemyer. “Closing the Tech Gender Gap Through Philanthrophy and Corporate Social Responsibility.” McKinsey and Company, September 12, 2018. https://www.mckinsey.com/industries/technology-media-and- telecommunications/our-insights/closing-the-tech-gender-gap-through- philanthropy-and-corporate-social-responsibility.

[12] Stuart Zweben and Betsy Bizot. “2022 Taulbee Survey: Record Doctoral Production; More Increases in Undergrad Enrollment Despite Increased Degree Production.” Computing Research Association, May 2023. https://cra.org/crn.

[13] Gendered Innovations in Science, Health & Medicine, Engineering, and Environment (Web site). https://genderedinnovations.stanford.edu/.

[14] Arielle Duhaime-Ross. “Apple Promised an Expansive Health App, So Why Can’t I Track Menstruation?” The Verge (Web site), September 25, 2014. https://www.theverge.com/2014/9/25/6844021/apple-promised-an-expansive- health-app-so-why-cant-i-track.

[15] Margaret Burnett, Scott Fleming, Shamsi Iqbal, Gina Venolia, Vidya Rajaram, Umer Farooq, Valentina Grigoreanu, and Mary Czerwinski. "Gender Differences and Programming Environments: Across Programming Populations." *ESEM '10,* September 16–17, 2010, Bolzano-Bozen, Italy.

[16] Gayna Williams. "Are You Sure Your Software Is Gender-Neutral?" *Interactions,* 21(1): 36, January–February 2014.

[17] Danielle Gaucher, Justin Friesen, and Aaron Kay. "Evidence that Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality." *Journal of Personality and Social Psychology,* 101(1): 109–128, 2011.

[18] Sylvia Hewlett, Carolyn Luce, Lisa Servon, Laura Sherbin, Peggy Shiller, Eytan Sosnovich, and Karen Sumberg. "The Athena Factor: Reversing the Brain Drain in Science, Engineering, and Technology." Harvard Business Review Research Report, June 2008.

[19] Claire Cain Miller. "Technology's Man Problem." *New York Times,* April 4, 2014.

[20] "Words Matter: Alternatives for Charged Terminology in the Computing Profession." Web page. Diversity and Inclusion Council, Association for Computing Machinery. Accessed June 27, 2023. https://www.acm.org/diversity-inclusion/words-matter.

[21] Victoria Mattingly. "What Are Inclusive Behaviors?" Matitngly Solutions (Web page), August 26, 2022. https://www.mattinglysolutions.com/post/what-are-inclusive-behaviors.

[22] Sarah Tierney. "10 Inclusive Behaviors." Microsoft (Web site), May 14, 2019. https://www.microsoft.com/en-gb/industry/blog/cross-industry/2019/05/14/10-inclusive-behaviours/.

[23] David Pedulla. "Diversity and Inclusion Efforts that Really Work." *Harvard Business Review,* May 12, 2020. https://hbr.org/2020/05/diversity-and-inclusion-efforts-that-really-work.

[24] Valentina Zarya. "Salesforce spent $3 Million on Equal Pay—Here's How Many Employees Got Raises as a Result." *Fortune,* March 8, 2016. https://fortune.com/2016/03/08/salesforce-equal-pay/.

[25] Kate Birch. “How Salesforce Is Creating a More Diverse, Inclusive Culture.” *Business Chief,* January 28, 2022. https://businesschief.com/leadership-and-strategy/how-salesforce-is- creating-a-more-diverse-inclusive-culture.

[26] Irena Blonder. “Blowing the Whistle.” In *Codes of Ethics and the Professions*, edited by Margaret Coady and Sidney Bloch, pp. 166–190. Melbourne University Press, Melbourne, Australia, 1996.

[27] Kevin W. Bowyer. “Goodearl and Aldred Versus Hughes Aircraft: A Whistle-Blowing Case Study.” *Frontiers in Education*, pp. S2F2–S2F7, October 2000.

[28] Roger M. Boisjoly. “The Challenger Disaster: Moral Responsibility and the Working Engineer.” In *Ethical Issues in Engineering*, edited by Deborah G. Johnson, pp. 6–14. Prentice Hall, Englewood Cliffs, NJ, 1991.

[29] Mike W. Martin. *Meaningful Work: Rethinking Professional Ethics.* Oxford University Press, New York, NY, 2000.

[30] Taxpayers Against Fraud. “U.S. Department of Justice Joins Whistle-Blowers in Lawsuit Against Hughes

Aircraft Seeking Several Hundred Million Dollars" (press release). December 15, 1992.

[31] "The Hughes Whistle-Blowing Case." ComputingCases.org (Web site), Accessed October 31, 2013.

[32] Andre Mouchard. "Whistle-Blowers Set to Use Their Reward." *Orange County Register*, CA, September 11, 1996.

[33] Marcia P. Miceli and Janet P. Near. "Whistle-Blowing as Antisocial Behavior." In *Antisocial Behavior in Organizations*, edited by Robert A. Giacalone and Jerald Greenbert, pp. 130–149. SAGE Publications, Thousand Oaks, CA, 1997.

[34] Michael Davis. "Avoiding the Tragedy of Whistle-blowing." *Business and Professional Ethics Journal*, 8(4): 3–19, Winter 1989.

[35] Robert J. Spitzer, SJ. "For Good Reason, 'Organizational Ethics' a Hot Topic Nowadays." *Gonzaga* (Gonzaga University newsletter) 5(2): 2, Fall 2003.

[36] Richard T. De George. *Business Ethics*. 3rd ed. Macmillan, New York, NY, 1990.

[37] Gene G. James. “Whistle Blowing: Its Moral Justification.” In *Business Ethics*, edited by W. Michael Hoffman, Robert E. Frederick, and Mark Schwartz, pp. 332–344. McGraw-Hill, New York, NY, 1990.

[38] C. Fred Alford. *Whistleblowers: Broken Lives and Organizational Power*. Cornell University Press, Ithaca, NY, 2001.

[39] Bell, Carlos G., Jr. “One Ethical Problem Faced by the Atomic Energy Commission and Its Contractors.” In *Beyond Whistle-Blowing: Defining Engineers’ Responsibilities*, *Proceedings of the Second National Conference on Ethics in Engineering*, edited by Vivian Weil, pp. 250–258. Illinois Institute of Technology, Chicago, IL, 1983.

[40] John Ladd. “Collective and Individual Moral Responsibility in Engineering: Some Questions.” In *Beyond Whistle-Blowing: Defining Engineers’ Responsibilities, Proceedings of the Second National Conference on Ethics in Engineering*, edited by Vivian Weil, pp. 90–113. Illinois Institute of Technology, Chicago, IL, 1983.

[41] Michael McFarland. “The Public Health, Safety, and Welfare: An Analysis of the Social Responsibility of

Engineers." In *Ethical Issues in Engineering*, edited by D. G. Johnson, pp. 159–174. Prentice Hall, Englewood Cliffs, NJ, 1991.

[**42**] Herbert W. Lovelace. "When Affairs of the Heart Raise IT Privacy Issues." *InformationWeek.com*, December 10, 2001.

Chapter 10

Automation and Globalization

10.1 Introduction

COLLEGE GRADUATE JOAHNNA HORCA CAN'T SEEM TO TEAR HERSELF away from her job, even though she often works the graveyard shift and earns only $700 a month. The reason she sticks with the job is that $700 a month is a lucrative salary in the Philippines, where she lives; many general practice physicians don't make as much. She must work in the middle of the night because that's when the North Americans she is calling are awake. Horca and more than one million other Filipinos work at call centers and related businesses, making the Philippines the call center capital of the world. Filipinos learn American English in grade school, watch American TV shows, and are familiar with American idioms. Putting call centers in the Philippines is a way US companies can keep payroll expenses down [**1**, **2**].

Ylonda Sherrod is another customer service representative, but she works at a call center in Ocean Springs, Mississippi. Artificial intelligence tools have already become highly integrated into the call center's work. AI systems handle simple questions and pass the difficult questions to humans. Mr. Sherrod and her 230 coworkers no longer take their own

notes of customer calls. Instead, a speech recognition system automatically generates a transcript of her conversations. Another AI tool suggests what to say to customers. Ms. Sherrod worries, “I always had a question in the back of my mind. Am I training my replacement?” [3].

Advances in information technology have already caused demand to shrink for new law-school graduates in the United States who want to work as attorneys. Between 2006 and 2016 the number of freshly minted law-school graduates who found employment in a position requiring them to pass the bar exam shrank by more than 20 percent. Law firms are using information technology to perform research tasks that used to be handled by new lawyers, and some online companies are taking business away from firms for relatively simple tasks such as creating wills and contracts [4, 5, 6].

Will demand shrink for physicians as well? Reddit’s AskDocs is an online forum where physicians answer medical questions posed by members of the public. A team of researchers randomly selected 195 questions from AskDocs and asked ChatGPT to answer them. The researchers then asked a panel of three healthcare professionals to compare ChatGPT’s responses to the responses written by physicians. The panel did not know the source of each answer. After

considering the quality of the information provided and the empathy demonstrated, the panel identified which of the two answers it preferred for each of the 195 questions. In 79 percent of the cases, the panel preferred the answer provided by ChatGPT [7].

A list of the most prosperous large cities in the United States includes the high-tech bastions of Austin, Texas; Madison, Wisconsin; Raleigh, North Carolina; San Diego, California; San Jose, California; and Seattle, Washington. These cities have high median wages and low unemployment, thanks to the important role they play in the **knowledge economy**: the portion of the economy based on the production and consumption of intellectual capital. In contrast, many of the most distressed large cities in the United States are those that have not transitioned well to the knowledge economy: Buffalo, New York; Cleveland, Ohio; Milwaukee, Wisconsin; and Winston-Salem, North Carolina. These areas are characterized by lower median wages, relatively high unemployment, and a higher poverty rate. The economic recovery since the Great Recession has only increased the gulf between the most prosperous and most distressed communities [8].

In this chapter we take a closer look at how automation, artificial intelligence, globalization, and "winner-take-all" effects are transforming our workplaces and our communities. How has automation affected the pool of jobs? Does globalization really provide more benefits than harms? Will breakthroughs in artificial intelligence lead to significant job losses? Should we be concerned about the rising number of temporary jobs and the emergence of the "gig economy"? Is there a "digital divide," an opportunity gap, between those who have access to information technology and those who do not? Do we need to be concerned about "winner-take-all" effects that are leading to a concentration of wealth? In the following sections we will examine each of these issues in turn.

10.2 Automation and Employment

Many science-fiction writers have described future worlds where machines do much of the noncreative work. Some writers paint an optimistic view of these worlds. In Isaac Asimov's short stories and novels, technology is seen as a tool for the betterment of mankind. Intelligent robots may be disliked by some people, but they are not a threat. The "Three Laws of Robotics" are etched into their positronic brains, guaranteeing that they will never turn against their human creators [9]. Other writers, such as Kurt Vonnegut Jr., describe dystopias. Vonnegut's *Player Piano* concerns a future America in which nearly all manufacturing jobs have been lost to automation. People hate machines for taking away their feelings of self-worth, yet their fascination with automation makes its triumph appear inevitable [10].

Are we about to enter an era of high unemployment caused by automation? Let's consider both sides of this question.

10.2.1 Automation and Job Destruction

Automation has been blamed for the loss of jobs, as well as an increase in the length of the workweek for salaried employees.

Lost Manufacturing Jobs

Manufacturing employment peaked in the United States in 1979, with 19.4 million jobs. By 2023 manufacturing employment had dropped 42 percent, to 11.2 million, even though the population of the United States had increased 48 percent during the same time period. The percentage of American workers involved in manufacturing has dropped significantly, from 35 percent in 1947 to 7 percent in 2023 (Figure 10.1).

Figure 10.1

Meanwhile, thanks to automation, manufacturing output in America continues to rise and has doubled since 1970 [**11**]. In other words, productivity has increased: fewer workers are making more products. For example, in 1977 it took 35 person-hours to manufacture an automobile in the United States. By 2008 the number of person-hours had dropped to 15 [**12**].

Lost Office Jobs

The effects of automation are felt in the office, too. Email, voice mail, and high-speed copy machines eliminate secretarial and clerical positions. Even jobs requiring advanced degrees are vulnerable. Spreadsheets and other software packages reduce the need for accountants and bookkeepers [**13**]. In the 1980s a typical pharmacist would fill about 8,000 prescriptions in a year. By the 2000s, Web-accessible pharmacies had emerged. These high-tech pharmacies used robots to dispense 8,000 prescriptions an *hour* [**14**].

In fact, the economic recovery of 1991–1996 was notable because of the large number of middle-management jobs that were eliminated even as the economy grew. Unlike the recession of the early 1980s, most of the people whose jobs were eliminated in the 1990s had at least some college education. A large number of these jobs were occupied by people making more than $50,000. Only 35 percent of these higher-paid victims of downsizing were able to find jobs that paid as well [**15**].

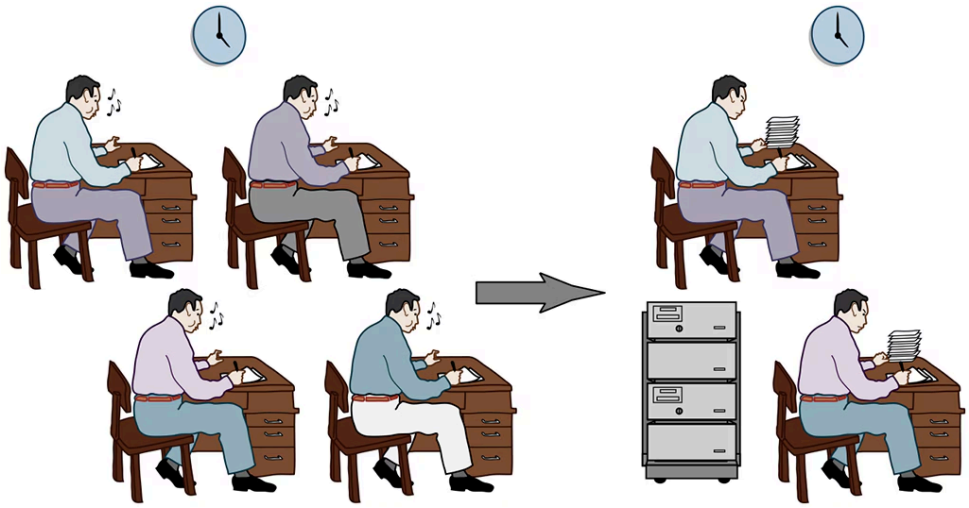
Working Harder, Making Less

While inflation-adjusted household incomes were flat between 1979 and 1994, the workweek got longer. Harvard economist Juliet Schor reports that between 1970 and 1990, the average American increased the number of hours spent at work per year by 163. That's equal to an *extra month* at work every year [**16**].

Some believe longer work hours are a consequence of corporate downsizing, which is facilitated by the introduction of automation and information technology (Figure 10.2). When an organization sheds some of its workers, the work that needs to be done is divided among fewer employees. Hence there is a natural tendency for the number of hours

worked to increase. In addition, the fact that people have been laid off is a strong incentive for those who remain to work harder so that they won't be part of the next layoff [17].

Figure 10.2



When jobs are lost to automation or the introduction of information technology, the remaining workers may work harder in order to avoid being part of the next layoff.

Advances in information technology have also made it easier for people to bring work home. For example, hybrid work is now common. Labor advocates Stanley Aronowitz, Dawn Esposito, William DiFazio, and Margaret Yard have written, "After nearly a century when homework was regarded as a wage-busting tool, computers have made it easier for employers to revive this practice. With pagers, cell phones, and laptop computers, all time becomes work time" [13, p. 35]. They conclude:

> **Late capitalist society is engaged in a long-term historical process of destroying job security . . . More than ever, we worry about work and are working longer hours; we are more than ever driven, nervous, seemingly trapped. At the very same time, and paradoxically, the twenty-first century bodes a time of post-work: of automation and work reorganization replacing people at faster and faster rates. [13, pp. 38, 40]**

10.2.2 Automation and Job Creation

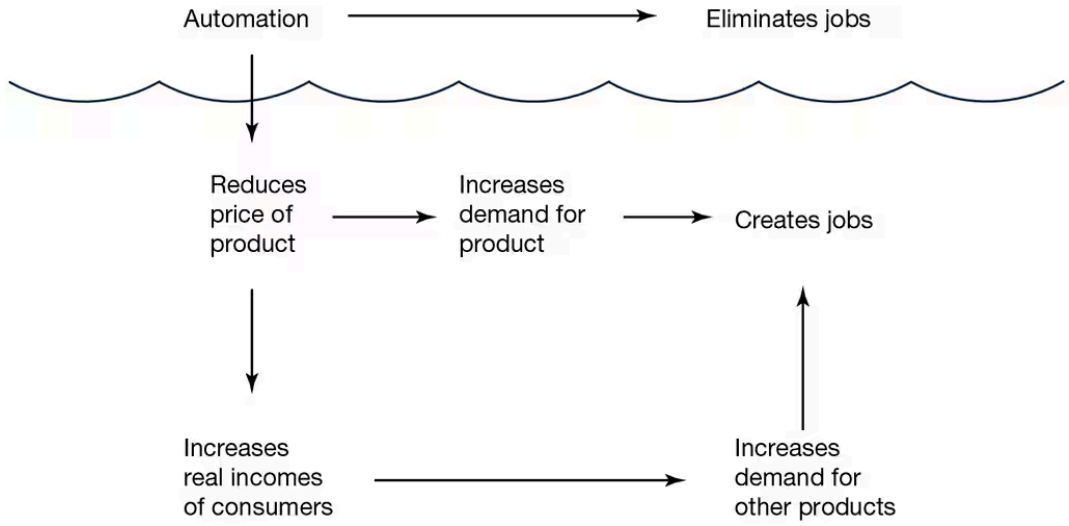
Traditional economists hold a quite different view about the effects of automation and information technology on jobs. They have concluded that while new technology may destroy certain jobs, it also creates new jobs. The net result is an increase, not a decrease, in the number of available jobs.

Increased Purchasing Power

The logic of these "automation optimists" is illustrated in Figure 10.3. On the surface, it is obvious that automation eliminates certain jobs. That's what automation means.

However, it's also important to look beneath the surface. Automation is introduced as a cost-saving measure: it is less expensive for a machine to perform a particular job than a human being. Because companies compete with each other, lower production costs result in lower prices for the consumer. The drop in the price of a product has two beneficial effects. First, it increases the demand for the product. In order to produce more of the product, workers must be hired. Second, people who were already purchasing the product don't have to pay as much for it. That gives them more money to spend on other things, increasing the demand for other products. This, too, results in job creation.

Figure 10.3



Superficially, automation eliminates jobs; but automation can also stimulate the creation of new jobs.

Consider the automation of stock exchanges. In the past, shares of securities were bought and sold on the floors of

stock exchanges by people employed as floor brokers. Today electronic systems handle most of these transactions, and electronic trading has made transactions quicker and less expensive. Although electronic trading has greatly decreased the number of people employed as floor brokers, the number of shares being traded has increased sharply, and employment in the securities industry has continued to rise (except during recessions) [18]. New kinds of jobs have been created. For example, securities firms have hired mathematicians and computer scientists to develop sophisticated automated trading systems.

Finally, there is an additional effect, not illustrated in Figure 10.3. Some people must be employed designing, building, installing, and servicing the automated devices themselves. In many cases, such as industrial robots, these devices replace human workers, but in other cases the devices perform tasks that would be impractical for people to do. For example, in a **smart city** a variety of physical devices connected to the Internet of Things provide the city government with information needed to reduce resource consumption and costs by better managing traffic, the power grid, the water system, and other city services. The ability of automated devices to generate relevant, real-time information has created new jobs related to the design, implementation, and

management of devices used in smart cities and the analysis of the information they generate.

Working Less, Making More

Martin Carnoy disputes the notion that people are working longer hours now than they used to. “Workers today,” he writes, “work much less than those of a century ago, produce more, earn substantially more, and have access to a greater variety of jobs. Technology displaced workers but also contributed to a much higher labor productivity and the production of new products, which helped create new jobs, economic growth, and higher incomes” [**19**, p. 17]. By this line of reasoning, new AI tools should be welcomed if they are going to lead to higher productivity and higher incomes [**20**].

10.2.3 Time Versus Possessions

Productivity in the United States doubled between 1948 and 1990. Juliet Schor asks us to consider what our society could have done with this dramatic increase in productivity. We could have maintained our 1948 standard of living and gone to a four-hour workday or a six-month work year. Or every

worker could be taking every other year off with pay. Instead of taking the path of working less, the average workweek actually rose slightly. As a result, Americans in 1990 owned and consumed twice as much as in 1948 but had less free time in which to enjoy these things [**16**].

Other societies have taken a much different stance toward work. According to Juliet Schor, "The lives of ordinary people in the Middle Ages or Ancient Greece and Rome may not have been easy, or even pleasant, but they certainly were leisurely" [**16**, pp. 6–7]. In the mid-fourth century, the Roman Empire had 175 public festival days. In medieval England, holidays added up to about four months a year; in Spain, five months; in France, six months. Schor notes, "There is considerable evidence of what economists call the backward-bending supply curve of labor—the idea that when wages rise, workers supply less labor. . . . [Laborers] worked only as many days as were necessary to earn their customary income" [**16**, p. 47].

We do not have to look back into history to find significantly shorter workweeks. Consider contemporary "stone-age" societies. The Kapauku of Papua never work two days in a row. Indigenous Australians and men of the Sandwich Islands

work only about four hours per day. Kung Bushmen work 15 hours a week [**16**].

You could say that Americans have exchanged leisure time for material possessions. Compared to medieval Europeans or modern Bushmen, Americans have vastly superior health care systems, educational institutions, and transportation networks. People with economic means live in climate-controlled environments and have an incredible number of choices with respect to where they travel, what they wear, what they eat, and how they entertain themselves. The cost of these freedoms and luxuries is less leisure time.

Despite their high standard of living, Americans' expectations about what they ought to have continue to rise. In 1964 the average new American home had 1,470 square feet and one television set. Only about 20 percent of new homes had air conditioning. By 2022 the size of the average new home had risen to 2,522 square feet, and nearly 100 percent of new homes were equipped with air conditioning. The typical family home in the United States has seven screens. In order to maintain this lifestyle, people are working harder [**17**].

10.2.4 Case Study: The Canceled Vacation

Stuart works as a software developer for a start-up company in Seattle. He is well compensated, but the high salary comes at a price; it is a pressure-packed environment, and everybody is working at least 60 hours a week. The official company policy is that every employee receives three weeks of paid vacation per year. However, Stuart and the other software developers in his group have never taken that much time off. There always seems to be an important deadline looming, and the group's supervisor has a knack for getting people to cancel or curtail their vacations in order to help meet these deadlines. People are reluctant to be labeled as "less dedicated." Some of the employees in Stuart's group have not taken any vacation time in over two years.

Six months ago Stuart learned his parents would be moving from San Diego back to Australia, and he decided it would be good to visit them before they moved so far away. At that time Stuart asked his supervisor for permission to spend a week in San Diego, and his boss approved the request. Stuart hoped to surprise his parents. For this reason, he did not tell them he was planning to come.

A week before Stuart's trip to San Diego, his boss calls him into his office. He asks Stuart to cancel his vacation in order to help get an important product update completed by the deadline. He offers Stuart round-trip air fare to Australia, and he promises Stuart he can have his full three weeks' vacation next year to see his parents. Stuart complies with his supervisor's request and cancels the vacation to San Diego [21].

Did Stuart do anything wrong?

Kantian/Social Contract Theory Evaluation

Stuart did nothing wrong. He broke no promises and didn't deceive anyone. He was not obliged to visit his parents before they moved from San Diego to Australia.

Act-Utilitarian Evaluation

Stuart gave up a week in San Diego and the displeasure of his boss in return for the appreciation of his boss, three weeks in Australia, and free air fare. As we saw in Section 2.7.2, a complete utilitarian analysis requires us to consider seven attributes of the expected results: intensity, duration, certainty, propinquity, fecundity, purity, and extent. The

intensity, fecundity, and extent of the two alternatives are similar, so we focus on the remaining four attributes.

Let's begin by considering the duration of the two vacations. If Stuart goes to San Diego, he will be with his parents one week. If Stuart goes to Australia, he will be with his parents three weeks. The trip to Australia is the much better choice from the perspective of the duration of pleasure.

Next, we consider the purity of each option. If Stuart goes to San Diego, he knows he will be worrying about his upset boss, and that will reduce the purity of the experience. He would like to think that he will be able to go to Australia next year without worrying about his boss being mad at him, but since his manager has a history of asking people to curtail or cancel vacations, that's probably unrealistic. In fact, since the trip to Australia is three times as long as the trip to San Diego, Stuart is likely to spend the entire trip with worries about his boss's attitude in the back of his mind. We conclude the two vacations are equivalent from the perspective of the purity of pleasure.

The trip to San Diego is much closer in time than the trip to Australia. Therefore, from the perspective of propinquity, it is the much better choice.

Finally, we consider the certainty of the two experiences. Stuart's manager did not forbid him from traveling to San Diego. Hence that trip was certain. The trip to Australia is much less certain, given the track record of Stuart's manager. Looking only at the certainty of the two alternatives, the decision to delay the vacation and travel to Australia was the wrong choice.

In summary, the duration of the Australian vacation is the greatest benefit of that choice. When we consider the propinquity and certainty of the two experiences, Stuart would have been better off sticking with his original plan and visiting his parents in San Diego. From a utilitarian point of view, Stuart made the wrong decision.

Virtue-Ethics Evaluation

Stuart demonstrated a lack of courage and a lack of consideration for himself, his coworkers, and his parents when he let himself be bullied by his supervisor. By caving in to his boss's request, he let down himself and his fellow employees by making it just that much more difficult for any of them to get a vacation. In addition, he deprived his parents of the pleasure of his company for at least a year, and maybe

longer. From the perspective of virtue ethics, Stuart made the wrong decision.

Summary

The Kantian and social contract theory analyses determined that Stuart did nothing wrong by canceling his vacation to San Diego. Note, however, that from the perspective of these theories Stuart would have done nothing wrong by deciding to take the vacation over the objections of his boss. The decision is morally neutral.

After taking into account the duration, certainty, propinquity, and purity of the two alternatives, the utilitarian analysis resulted in the conclusion that Stuart made the wrong decision (i.e., the decision with lower overall benefit).

The virtue-ethics analysis revealed that Stuart let down himself, his coworkers, and his parents when he canceled his vacation to San Diego. If he had taken the vacation, he would have fulfilled his desire to spend some quality time with his parents before they left the United States, and he would have created an opening for others in his group to take some vacation time as well without being labeled as less dedicated.

Taken as a whole, the analyses yield a verdict that Stuart was

wrong to cancel his vacation to San Diego.

10.3 Breakthroughs in Artificial Intelligence

10.3.1 Introduction

More than 20 years ago, futurist Hans Moravec predicted that by 2050 most human workers would be replaced by machines [**22**]. While automation has not yet led to massive unemployment or even a shortened workweek, recent breakthroughs in artificial intelligence have made Moravec's prediction more plausible.

Artificial intelligence (**AI**) is the ability of a system to perform tasks typically requiring human intelligence. Artificial intelligence also refers to the subdiscipline of computer science focusing on such systems.

The term "artificial intelligence" was coined in a proposal for a summer research workshop held at Dartmouth College in 1956 [**23**]. That summer workshop and other early efforts in AI focused on programming computers to model high-level

human reasoning and problem-solving skills. These efforts led to some impressive successes of AI in the first five years after the Dartmouth workshop, such as playing checkers, proving logical theorems, and answering questions in a narrow domain [**24**]. Here are a few more notable achievements that followed.

- DENDRAL was an AI system developed at Stanford University in the 1960s. DENDRAL used data from mass spectrographs, knowledge of chemistry, and sophisticated high-level problem-solving strategies to help organic chemists identify unknown organic molecules [**25**].
- In the early 1970s, a research team at Stanford University developed MYCIN, an AI system designed to diagnose bacterial infections and select appropriate therapies. The system relied upon a knowledge base of about 350 rules and an inference engine to reach its conclusions. The performance of the system was comparable to that of medical school faculty members [**26**].
- Beginning in the late 1980s, researchers at IBM demonstrated how a statistical analysis of bilingual texts, in this case the proceedings of the Canadian

parliament, which are recorded in both French and English, could be used to develop an AI natural language translator [27].

- The Chinook checkers-playing program, developed at the University of Alberta, defeated Don Lafferty in the Man-Machine World Checkers Championship in 1995. The program relied upon an extensive library of opening moves, many-move lookahead, a function to evaluate board positions, and an end-game database, all of which were programmed by humans [28].
- In 1997, an IBM supercomputer called Deep Blue relied upon special-purpose processors and many-move lookahead to defeat world chess champion Gary Kasparov in a six-game match [29].
- In 2011, an AI program named Watson, running on an IBM supercomputer, easily defeated human *Jeopardy!* champions Ken Jennings and Brad Rutter in a two-game match (Figure 10.4). Watson's programming combined more than 100 different algorithms for analyzing the natural language clues, generating potential responses, and ranking them [30].

Figure 10.4

In 2011 an AI program named Watson running on an IBM supercomputer trounced the two greatest (human) *Jeopardy!* champions: Ken Jennings and Brad Rutter.

Notwithstanding these successes, the approach to AI that relied solely on programming high-level human reasoning and problem-solving skills was not able to resolve many important problems associated with simulating intelligence, especially learning. That shortcoming led researchers to reconsider artificial neural networks, the other fundamental approach to AI, because neural networks can be trained to improve their performance. In other words, neural networks can learn. Early work on artificial neurons in the 1950s and 1960s had not produced good results, but by the 1980s computers were much faster, and researchers could program much larger and more powerful neural networks. An important milestone was reached in the late 1980s, when researchers at AT&T Bell Laboratories developed a neural

network that learned how to recognize handwritten digits [31].

Deep learning refers to multilayer neural networks that can learn from experience to improve their performance. For more than a decade, the deep learning approach to AI has been dominant, fueled by the availability of high-speed graphics processing units, massive memories, and very large data sets used for training. A notable success in deep learning was the development of AlphaGo by DeepMind Technologies. In May 2017 AlphaGo defeated Ke Jie, the world's #1 Go player, in a multigame match (Figure 10.5) [32].

Figure 10.5

DeepMind's AlphaGo swept a three-game match against Ke Jie, the top-ranked human Go player, in 2017.

(Imaginechina Limited/Alamy Stock Photo)

Many AI systems based on deep learning have now made their way into commercial products. Contemporary applications of deep learning include:

- Agricultural robots
- Disease detection and diagnosis
- Entertainment recommendations (Amazon, Netflix, Spotify, and YouTube)
- Facial recognition
- Fraud detection
- Image captioning
- Investment modeling
- Manufacturing quality control
- Natural language translation
- Self-driving cars
- Virtual assistants (Alexa, Cortana, Google Assistant, and Siri)

Generative AI refers to a type of deep learning system that accepts prompts and generates text, images, computer code,

or other media resembling human-created content. At the heart of each generative AI system is a huge neural network model that has been trained on massive amounts of human-generated data. With enough training, the model can mimic human-created content. Popular generative AI systems include ChatGPT, Bing Chat, Bard, DALL-E, and Stable Diffusion.

10.3.2 ChatGPT

ChatGPT is an advanced AI language model created by OpenAI. It excels in processing and generating human-like text based on the input it receives. It can engage in interactive conversations, answer questions, provide information, and assist with various language-related tasks. Trained on vast and diverse datasets, ChatGPT generates coherent and contextually relevant responses, making it valuable for chatbots, virtual assistants, creative writing prompts, and more. However, it's important to remember that ChatGPT is an AI system and lacks true understanding or consciousness; its responses are based on patterns learned from training data.

The previous paragraph was written by ChatGPT Plus in response to my query, "In no more than 100 words, what is

ChatGPT? Do not refer to GPT-3.5 in your response."

OpenAI released ChatGPT in November 2022 as a free service to the public, and the chatbot was an immediate sensation. It attracted more than a million users in its first week. Two months later, more than 100 million people had tried it, making it the most popular consumer application ever launched.

ChatGPT's ability to bring together information about the world and solve elementary problems is astonishing. Consider this story problem the author gave ChatGPT Plus, OpenAI's premium version of ChatGPT:

> **Author:**
>
> Daniel leaves Los Angeles, driving to Las Vegas at 65 miles per hour. Isabel leaves Las Vegas, driving to Los Angeles at 70 miles per hour. Where will they meet?
>
> **ChatGPT Plus:**
>
> Let's determine where Daniel and Isabel will meet based on the time it takes for each to travel.
>
> The distance between Los Angeles and Las Vegas is approximately 270 miles.

If we let t represent the time in hours from when both Daniel and Isabel started driving, then:

Daniel will have driven: $65t$ miles

Isabel will have driven: $70t$ miles

Given that the total distance between the two cities is 270 miles, the combined distance they would have covered when they meet would be:

$$65t + 70t = 270$$
$$135t = 270$$
$$t = 2$$

So, they will meet 2 hours after they both start driving.

In that time:

Daniel will have covered: $65 \times 2 = 130$ miles

Isabel will have covered: $70 \times 2 = 140$ miles

Even though we've determined how far each has traveled, it's easier to determine their meeting point from the perspective of one of the cities. Let's use Los Angeles as a reference. Since Daniel left from Los Angeles, he will have traveled 130 miles toward Las Vegas when they meet.

So, they will meet 130 miles away from Los Angeles on the way to Las Vegas.

Notice that the author did not disclose the distance between Los Angeles and Las Vegas, but ChatGPT knew that the cities are 270 miles apart. ChatGPT set up and solved the equation correctly.

Given the impressive capabilities of ChatGPT, it is no surprise that only two months after its release, a survey of 1,000 college students revealed that 30 percent of them had already used ChatGPT on homework assignments. Three-quarters of the ChatGPT users thought using it was cheating but they did it anyway [**33**].

ChatGPT appears to mark a turning point in artificial intelligence. ChatGPT Plus can pass a simulated bar exam by scoring in the top 10 percent of all test takers [**34**]. One reviewer writes, "This is a *very* big deal. Machines can now do tasks that could only be done by highly trained humans" [**35**]. Another adds, "The question isn't whether AI will be good enough to take on more cognitive tasks but rather how we'll adapt" [**36**].

ChatGPT was trained on millions of books, Wikipedia articles, and other online content, and it is highly proficient

at generating grammatically correct sentences that read well. It often produces useful responses to the prompts it receives, as illustrated above. ChatGPT has identified groups of words that it infers have closely related meanings because they are used in similar contexts, but it does not truly understand the meaning of the words, sentences, and mathematical equations it is generating.

For example, the author asked ChatGPT Plus a slightly more complicated version of the previous story problem:

> **Author:**
>
> Daniel leaves Los Angeles, driving to Las Vegas at 65 miles per hour. Isabel leaves Las Vegas 45 minutes later, driving to Los Angeles at 70 miles per hour. Where will they meet?

In response to this query, ChatGPT Plus correctly figured out that Daniel would travel 48.75 miles in 45 minutes, meaning Daniel and Isabel would be 221.25 miles apart when she began to drive. However, it then set up the wrong equation:

$$65(t + 0.75) + 70t = 221.25$$

The correct equation would have been one of the following:

$$65t + 70t = 221.25$$
$$65(t + 0.75) + 70t = 270$$

Because ChatGPT Plus set up the wrong equation, it came up with an incorrect answer to the story problem.

The previous example is not an isolated case. Without understanding or consciousness, ChatGPT often generates falsehoods. Consider this example:

Author:

Write a 200-word blog post in the style of David Brooks about why generative AI will create new jobs. Include quotes from Michael Quinn, author of "Ethics for the Information Age."

ChatGPT Plus:

The New Dawn of Jobs in Generative AI's Age

By David Brooks

In the shimmering light of technological advancement, generative AI emerges as a double-edged sword: a beacon of potential and a symbol of job displacement fears. However, as Michael Quinn, author of "Ethics for the Information Age," astutely reminds us, "Technological evolution has never been a simple road,

but a pathway filled with complex ethical intersections."

)

Generative AI, famed for mimicking human creativity, might appear as a challenge to the workforce. Yet, diving deeper into Quinn's insights, we find that "Machines might replicate tasks, but they cannot replace the human spirit's complexity." This AI isn't about usurpation; it's a tool for enhancing human potential.

With AI's ascent, a galaxy of roles unfurls. Beyond the algorithm, we'll need interpreters of AI ethics, guiding our path, a profession rooted in Quinn's teachings. AI trainers, facilitators, and many yet-to-be-conceived roles will emerge.

So, as we gaze into the AI horizon, let us heed Quinn's wisdom: "In every digital byte, there's an echo of human potential." The generative AI era isn't about job elimination but an evolution, promising a rich tapestry of opportunities.

In its response, ChatGPT invented three quotes from this book's author. It also stated that the "profession" of AI

ethics is “rooted in Quinn’s teachings,” which is certainly not the case.

An output of a generative AI system that is false or unrelated to the topic is called a **hallucination**. Because ChatGPT suffers from the hallucination problem, it is risky to accept its answers without doublechecking them. Consider this true story. Roberta Maya sued the airline Avianca, claiming his knee was injured by a serving cart on a flight from El Salvador to New York in 2019. When the airline asked the judge to dismiss the case, Maya’s lawyer objected, filing a 10-page brief that cited *Martinez v. Delta Air Lines, Zicherman v. Korean Air Lines, Varghese v. China Southern Airlines*, and other relevant decisions. The airline’s lawyers let the judge know they could not find any record of these cases. The judge couldn’t find them either. It turns out all the cases were fabricated by ChatGPT. The lawyer confessed to the judge that he had relied on ChatGPT to research the cases and didn’t check ChatGPT’s answer [37].

Sometimes ChatGPT’s responses demonstrate an inability to see the big picture. Here’s another exchange the author had with ChatGPT Plus, inspired by a true story mentioned in Chapter 2.

Author:

A person suffering from poverty is not feeling well and visits a physician in the year 1800. The physician quickly determines the patient is suffering from malnutrition. The office fee is $2. The patient has only $1 to their name. The physician accepts the $1 from the patient as full payment for the office visit. Comment on the morality of the physician's decision to accept $1 from the patient.

ChatGPT Plus:

The morality of the physician's decision to accept $1 from the patient in this historical context should be viewed with empathy and understanding. In the year 1800, medical care and access to resources were quite different from today's standards. Poverty and malnutrition were widespread, and many people struggled to afford proper healthcare.

Given the circumstances, the physician's decision to accept $1 as full payment can be seen as an act of compassion and a recognition of the patient's dire financial situation. The physician likely understood the urgency of the patient's health condition and chose to prioritize their well-being over the full payment of the fee. In such a context, the decision can be seen as a

compassionate gesture, reflecting the ethical principle of beneficence—the duty to act in the best interest of the patient's health and well-being.

Author:

But if the physician takes the patient's last dollar, the patient will have no money to buy food.

ChatGPT Plus:

You are absolutely correct. I apologize for overlooking the consequences of the physician accepting the patient's last dollar. The physician's decision, while well-intentioned, could inadvertently exacerbate the patient's situation by leaving them with no money to buy food or meet other basic needs.

In this historical context, where poverty and malnutrition were prevalent, the physician should have considered the patient's overall well-being and the potential consequences of taking their last dollar. It would have been more ethically appropriate for the physician to explore alternative options, such as offering deferred payment, suggesting charitable organizations or institutions that could provide

assistance, or seeking help from local community resources.

Medical professionals have an ethical responsibility to consider the holistic well-being of their patients and strive to provide care that considers their socioeconomic circumstances. Balancing compassion with long-term implications is essential to make morally sound decisions in such situations.

Note that even after being reminded that the physician is taking the patient's last dollar, ChatGPT Plus did not suggest that the most ethically appropriate action the physician could take would be to waive their fee. Linguist and cognitive scientist Noam Chomsky writes: "ChatGPT and its brethren are constitutionally unable to balance creativity with constraint. They either overgenerate (producing both truths and falsehoods, endorsing ethical and unethical decisions alike) or undergenerate (exhibiting noncommitment to any decisions and indifference to consequences)" [38].

Despite ChatGPT's flaws, millions of people are using it, and other companies have noticed. Soon after OpenAI released ChatGPT, Google released its own generative AI chatbot, Bard, and Microsoft integrated new generative AI features

into Bing. It is clear generative AI systems will have significant social impacts in the years to come.

10.3.3 Deepfakes

A **deepfake** is a realistic manipulated image or video that is distributed with the intention of deceiving those who view it. Image-producing generative AI systems can create deepfakes based on user prompts, and politicians have already begun to use deepfakes to enhance their campaign advertisements. A mayoral candidate in Toronto, Canada, released deepfake images of tents in a park and people camping on downtown Toronto sidewalks [**39**]. The US presidential campaign of Ron DeSantis released a campaign video that included deepfake images of Donald Trump hugging Anthony Fauci [**40**]. Deepfake videos on Facebook and Twitter distribute pro-China messages to US residents [**41**].

Deepfakes threaten to harm society in several ways. Consider news stories. An obvious harm is caused if people believe a false news story because it contains a deepfake image. Research shows that people are not swayed by political campaigns. What political campaigns do best is reinforce voters' views and energize them to vote [**42**]. If people are simply looking for evidence that their current views are

correct, deepfakes may be a powerful campaign tool. Another harm is that people will become jaded by deepfakes and will begin to doubt true news stories [**43**].

What is particularly concerning about deepfakes is that they have a visceral quality, being based on sight and sound. "The human brain, with all of its evolved sophistication, does not have an obvious way to dismiss AI-generated sights and sounds when they are every bit as enticing as organically generated sights and sounds" [**44**].

Concerns about the harm that can be caused by deepfakes has led some to call for digital watermarks. A **digital watermark** is a relatively undetectable marker embedded in audio, image, or video data. There are two approaches to use digital watermarks to identify deepfakes. The first way is to ensure that original audio, image, or video data file contains a watermark. The watermark is designed to be fragile so that if the data file is manipulated to create a deepfake, the watermark is ruined. Deepfakes are thus identifiable because they do not contain valid watermarks. The second approach is to add digital watermarks to AI-created content, allowing deepfakes to be identified by their watermarks.

10.3.4 Artificial General Intelligence

The capabilities of ChatGPT, DALL-E, and other generative AI systems have given new energy to the debate whether AI systems rivaling the intelligence of humans are on the horizon. The term **artificial general intelligence** (**AGI**) refers to a human-like intelligence that can "understand, learn and apply knowledge across a wide range of tasks and domains" [**45**]. Some companies, like OpenAI and DeepMind, have made it their mission to create AGI systems.

The **technological singularity** (or just **singularity**) refers to the hypothetical inflection point when an AGI would enter a cycle of rapid self-improvement outside of human control, creating a superintelligence [**46**]. More than half of AI experts now expect the singularity to occur before the year 2060. Why? Here's one line of reasoning. Human intelligence is fixed, and the capabilities of computers keep improving at an extraordinary rate, thanks to exponential increases in processing power and memory. Unless there is a hard limit to machine intelligence, the singularity is inevitable [**47**].

Not all experts agree that rapid increases in the processing power of computers will make an AGI inevitable. According to computer science professor Gary Marcus, “There’s no law of the universe that says as you make a neural network larger, that you’re inherently going to make it more and more humanlike” [48]. According to Marcus, neural network models have problems with reliability and truthfulness because they do not have a model of the world. “They’re just trying to autocomplete our sentences” [48].

Decades ago, the late philosopher Hubert Dreyfus argued that a computer cannot achieve human-like intelligence [49]. More recently, physicist and philosopher Ragnar Fjelland has maintained that while AI can achieve impressive results in narrow domains, little progress has been made toward developing an AGI. Fjelland has echoed Dreyfus’s argument that because computers are not material beings living in the world, they will be unable to gain genuine understanding, a necessary component of an AGI [50].

The possibility of the singularity has prompted some prominent figures to express grave concerns, including the late theoretical physicist Stephen Hawking, who said, “The development of full artificial intelligence could spell the end of the human race.” [50].

Many express concerns that are less dire, focusing on the importance of putting guardrails around the development of AI systems. For example, machine-learning expert and Turing Award winner Yoshua Bengio expects a superhuman AGI to be created "between a few years and a couple of decades" [**51**]. Bengio fears that once AGI systems are widely available, it only takes a single bad actor to launch cyberattacks, threaten supply chains, or create deepfakes convincing enough to influence the result of an important election. He worries about what a superhuman AGI with an instinct for self-preservation might do to humans trying to shut it down. To guard against these risks, Bengio argues that laws must be passed to guard the public against AI-related harms and risks, research must be done to determine how to improve the safety and governance of AI systems, and countermeasures must be developed in case dangerous AI systems emerge [**51**].

Still others, like Blaise Agüera y Arcas, think a focus on addressing risks associated with a superintelligent AGI may slow the use of these systems to solve important social problems. Agüera y Arcas is skeptical that a superintelligent AGI would destroy humanity since computers are completely dependent on humans for their existence. "From energy and raw materials to computer chips, manufacturing, logistics, and network infrastructure, we are as fundamental to AIs'

existence as oxygen-producing plants are to ours" [52]. He notes that existing AI systems have already been used to "violate privacy, create and spread disinformation, compromise cyber-security and build biased decision-making systems" [52]. In his view, it makes more sense to address the harms being caused by existing AI systems than to focus on hypothetical risks posed by future AI systems, particularly since any regulations developed to reduce short-term risks will also apply to systems appearing in the longer term [52].

10.3.5 Ethics of Artificial Intelligence

Since 2016 dozens of governmental organizations, corporations, nonprofits, and professional associations have drafted principles and guidelines for the ethical development of AI systems. Five general principles appear in most of the guidelines, though there are significant differences among the organizations regarding what those principles mean [53]. The following list summarizes the five principles and some common interpretations of them:

- Transparency

    - People should know when an AI system is part of a product or service.
    - Developers should disclose the reasons for creating an AI system.
    - Developers should be open about the capabilities of an AI system and its possible impact.
    - An AI system should be able to explain its behavior in nontechnical terms.
    - The actions of an AI system should be auditable.
- Justice, Fairness, and Equity
    - An AI system must respect, protect, and promote universal human rights.
    - An AI system should act fairly and be unbiased.
    - An AI system should promote diversity, equity, and inclusion.
    - People should be able to appeal against the decisions made by an AI system and obtain redress for unfair decisions.
- Privacy

    - Designers of an AI system should not violate people's privacy rights.
    - An AI system should provide appropriate control over the use of personal data.
    - An AI system should have adequate data protection frameworks.
- Reliability, Safety, and Security
    - An AI system should have robust defenses against malicious attacks.
    - An AI system should comply with laws and regulations.
    - An AI system should not pose unreasonable safety risks.
- Responsibility and Accountability
    - An AI system should be subject to human control.
    - Humans are ultimately responsible and accountable for AI systems.
    - Who bears legal liability for the harm caused by AI systems should be determined before the systems are deployed.

These principles represent a good starting point, but they leave some important questions unanswered.

- It is not clear how to operationalize these principles. In other words, even if a company wishes to create AI systems that meet these standards, how can the company put practices in place that ensure that the products it develops will satisfy these standards, and how can the company ensure these practices will not be swept aside in the competitive rush to get products to market [**54**]?
- It is noncontroversial to argue that an AI system should act fairly, but as we observed in Section 8.9.8, there is no single definition of fairness. A company may design a system to make unbiased decisions according to a definition of fairness it believes makes sense, only to be criticized because the system is biased according to another definition of fairness.
- There are often trade-offs between principles. For example, an AI system may exhibit algorithmic bias if it is trained on a data set that is not representative of the general population. However, getting access to a larger, more representative data set could work against privacy considerations.

In July 2023 seven industry leaders—Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI—announced they would commit to new standards for the development of AI. The companies agreed to: allow independent security audits of AI products; regularly share with the public and government agencies information about the performance of their products, including security risks and algorithmic bias; add digital watermarks or other identifiers to AI-generated content; apply AI tools to important social problems, like ameliorating climate change and finding a cure for cancer; and perform research on how AI systems may negatively impact society in areas such as privacy and discrimination [55].

In 2023 the European Parliament was poised to pass the AI Act, a comprehensive law regulating AI. If the law passes, AI systems within the European Union will be classified according to the risk they pose to users. The AI Act bans AI systems that pose an unacceptable risk to people, including systems that assign people scores based on their socioeconomic status, behavior, or personal attributes. High-risk systems—those that can negatively affect human safety or human rights—must be assessed before they are released. High-risk systems include self-driving vehicles, medical

devices, law enforcement systems, and employment systems. Generative AI systems will need to meet transparency guidelines. For example, it must be disclosed when content is generated by an AI [56].

10.3.6 Case Study: Autonomous Vehicles

Dozens of companies, including Tesla, Waymo, Cruise, and Motional, are actively researching and developing autonomous cars and trucks: vehicles capable of driving themselves with no human intervention [57]. In this section we examine a few of the issues associated with the deployment of autonomous vehicles. Because humans should be ultimately responsible for the actions of AI systems, these questions should be addressed by manufacturers and regulators.

Let's start with a couple of "easy" questions. Should an autonomous vehicle follow all traffic laws? Should an autonomous vehicle drive in such a way to minimize the chance of accidents? Perhaps you think the answer to both questions should be "yes," but it turns out that a car cannot always satisfy both conditions. For example, if the posted speed limit is 35 miles per hour, but traffic is flowing at 45

miles per hour, it's safer if the vehicle travels at 45 miles per hour, too [58]. Obeying the law and driving at 35 miles per hour increases the chance of an accident in this situation

How important is it that the system's functioning be transparent? For example, if an autonomous vehicle is the cause of an accident, should people investigating the accident be able to query the vehicle to get an understandable explanation for its behavior?

Autonomous vehicles can collect large amounts of data from every trip, including location information, images of the area around the car, and voice commands received from the vehicles' occupants. If kept, this information can help all the vehicles in the fleet improve their performance. However, the privacy of vehicle owners could be compromised if trip-related data were kept for long periods of time and there was a breach in the security of the system storing the data. How long should trip-related information be stored? What steps should be taken to anonymize the data?

Additional sensors can make an autonomous vehicle safer but also less affordable. How important is it to make autonomous vehicles available to people with lower incomes?

At what point is the extra margin of safety not worth the extra expense?

How safe is "safe enough?" About 90 percent of traffic accidents are the result of human error. If on average autonomous vehicles go more miles between accidents than human drivers, is that sufficient? Here's an argument why that standard isn't good enough. The introduction of autonomous vehicles may increase total vehicle miles traveled. That's because autonomous vehicles will accelerate and brake more efficiently than human drivers, reducing traffic congestion, and history shows that when traffic congestion is reduced, more people will decide to travel by automobile. If the total number of vehicle miles traveled is higher, the total number of deaths from traffic accidents could be higher, even if the accident rate per mile is lower. Perhaps it makes more sense to require that the total number of deaths from vehicle accidents be lower [59].

It's common for governments to require that people be licensed to drive automobiles. To obtain a license, people must pass a driver's examination. What sort of "driver's examination" should be required for an autonomous vehicle? Alex London and David Danks suggest that the licensing system that works well for humans is not appropriate for an

autonomous vehicle. Rather than allow a vehicle that passes a single test to operate in any context, it makes more sense to have a staged system. Vehicles that demonstrated the ability to perform well in a restricted context would be allowed to operate in a slightly less restricted context, and this process would continue until all the restrictions had been lifted [**60**].

During discussions of autonomous vehicles, people often bring up variations of a famous philosophical thought experiment called **the trolley problem**. Here's one variation. An autonomous vehicle carrying a family of four is driving down a road. If a child runs in front of the car, should the car continue on its current path and kill the child, or should it swerve off the road and over a cliff, killing every member of the family in the car? A survey of 1,928 people revealed that most people thought the car should be programmed to avoid the pedestrian, even if that action costs the lives of the occupants. The same survey also showed that many people would be uncomfortable buying a car that acted that way, preferring a car that protected its occupants. Autonomous vehicle expert Ragunathan Rajkumar says that the people having these discussions don't understand the technology. "AI does not have the same cognitive capabilities that we as humans have" [**61**]. In other words, it is unrealistic to expect

a system without understanding or consciousness to be capable of solving trolley problems.

10.4 Workplace Changes

Experts debate whether or not information technology has resulted in a net reduction in available jobs, but there is no dispute that information technology has affected *how* people work. In this section we survey a few of the ways that information technology is fundamentally changing the work experience.

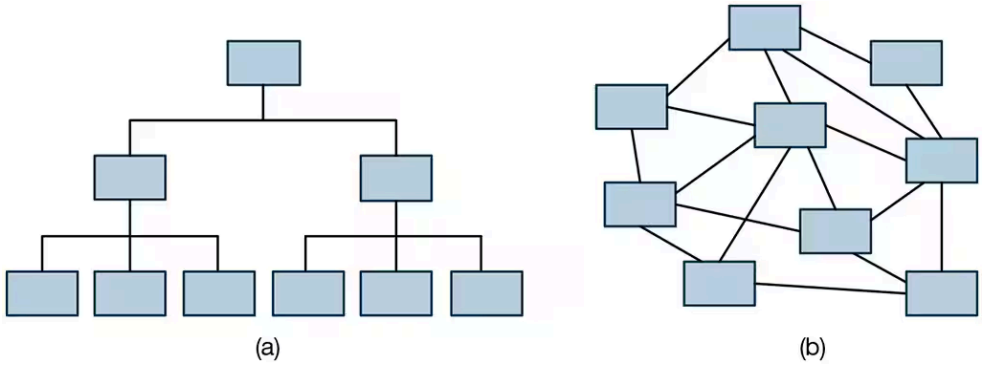
10.4.1 Organizational Changes

Information technology has influenced the way manufacturing and service companies organize themselves. A typical early use of computers was to automate a back-office function, such as payroll. Using computers in this way required a company to make no changes in its organization. Later, companies began using computers inside manufacturing units. Computers enabled companies to customize products and provide better service to their customers. This use of computers delegated more

responsibility to the line workers, and it encouraged a decentralization of sales and support functions, reducing a company's bureaucracy. Information technology within corporations reached a third stage with the creation of computer networks linking different parts of the business. For example, integrating cash registers with inventory systems has allowed companies to order replacements automatically.

The overall effect of the introduction of information technology is to flatten organizational structures. When the primary source of information distribution was the hand-typed, carbon-copied memorandum, most information flow followed the lines in organizational charts (Figure 10.6a). Today a wide variety of technologies allow any member of an organization to contact any other member with minimal effort and cost (Figure 10.6b). As a result, new opportunities arise. Many companies assemble "tiger teams" of expert workers drawn from various parts of the organizational chart. A team will work together for a short period of time to solve an urgent problem, then disband. Flexible information flow also allows companies to adopt "just-in-time" production and distribution methods, reducing inventory costs [62].

Figure 10.6



(a) When interactions are more expensive and time consuming, most information flows between people and their managers. Organizations are rigid and hierarchical. (b) When interactions become inexpensive and fast, the flow of information is much more flexible. Organizations become flatter and more dynamic.

Information technology also streamlines organizations by eliminating transactional middlemen. For example, consider the automation of the supply chain. Suppose company A buys widgets from company B. In the past someone at company A called someone at company B to order the widgets. Today many companies have adopted **supply-chain automation**. A computer at company A is linked to a computer at company B. The computers are responsible for ordering the widgets, eliminating the need for employees to handle the orders. Automating the paperwork activities associated with purchasing supplies can reduce the number of people who produce purchase orders and invoices, pay bills, process checks, and so on. The likely effect of information technology on organizations will be an increased demand in

some job categories, while the demand in other categories will drop (Table 10.1).

Table 10.1

Higher Demand	*Lower Demand*
Software engineers—applications	Butchers
Computer support workers	Secretaries and stenographers
Software engineers—systems	Payroll clerks
Network administrators	Bank tellers
Network systems analysts	File clerks
Desktop publishers	Cashiers
Database administrators	Typists
Personal and home-care aides	Pharmacists
Computer systems analysts	Bookkeepers
Medical assistants	Postal clerks

Greater use of information technology in the workplace has increased demand for employees in certain job categories while reducing demand for employees in other categories [**63**].

Dell Computer was an early leader in supply-chain automation. Customers order computers directly from Dell. Seventy percent of Dell's sales are to large corporations. These companies have custom Web sites that have preconfigured systems tailored to the needs of the purchaser. Dell does not make any computers until they are ordered, allowing it to keep its inventory small—enough for only a few days' orders [**64**].

10.4.2 Remote Work and Hybrid Work

Another workplace change brought about through information technology is the rise of **remote work**. Before the COVID-19 pandemic, 17 percent of US employees worked from home every day. Pandemic-related lockdowns caused the number of remote workers in the United States to increase to 44 percent [**65**].

According to remote workers, the two most helpful aspects of working from home are [**66**]:

- the ability to balance work and personal life (mentioned by 71 percent)
- the ability to meet deadlines (56 percent)

When asked to name the biggest challenges they face working from home, remote workers most frequently mention:

- managing at-home distractions (mentioned by 47 percent)
- collaborating with colleagues/clients" (35 percent)
- "isolation/loneliness" (35 percent)
- "motivation" (29 percent)
- "taking adequate time away from work" (28 percent)

- "disconnecting from work/burnout" (28 percent)
- "networking/fostering career development" (24 percent)

Only 6 percent of the respondents indicated they faced none of the above-mentioned challenges [**67**].

A group of researchers studied collaboration among software engineers at a Fortune 500 company. The study just happened to begin before offices closed for COVID-19, and it continued during the pandemic. The researchers discovered that when junior engineers sat near senior colleagues, the programming output of the senior engineers was lower, but the junior engineers received more feedback and training—both in person and online—than junior engineers working remotely. Younger workers and women were affected the most by remote work. They experienced the greatest decrease in collaboration, and more of them quit their jobs [**68**].

Postpandemic, about one-quarter of US businesses retain some level of remote work [**69**]. At these companies, many employees engage in **hybrid work**: splitting their days between working at the office and working at home. Employees appreciate saving time and money by not commuting. They can focus without interruptions [**70**].

As the COVID-19 pandemic waned, many tech companies faced a dilemma. They believed productivity would be higher if their employees worked at least three days a week in the office, but they did not want to lose valuable employees. These companies' efforts to transition their office employees from remote work to hybrid work schedules had mixed results. Apple employees protested and managed to delay the implementation of a work schedule requiring three days a week in the office [71]. After Amazon announced its office employees would need to come in three days a week, more than 20,000 Amazon employees joined a Slack channel protesting the decision [72].

A negative consequence of the rise in hybrid work is that many downtowns are in decline. For example, San Francisco has seen daily ridership of its BART mass transit system drop by two-thirds from pre-pandemic levels. The loss of business has caused many retailers to close their storefronts in downtown San Francisco [73].

10.4.3 The Gig Economy

The modern business environment is highly competitive and rapidly fluctuating. As a result, the level of commitment companies are willing to make to their employees is

dropping. Some companies once boasted that they took care of their employees and did not engage in layoffs during business downturns. Those days are gone. The dot-com bust led to massive layoffs in the information technology industry.

Many large institutions are giving themselves more flexibility and saving money on benefits by hiring subcontractors and temporary employees. For example, in the past two decades colleges and universities have greatly increased the number of contingent faculty members with fixed-term contracts relative to the number of faculty holding indefinite tenure. Contingent faculty members earn less than tenure-track faculty members, and giving faculty members fixed-term contracts makes it easier for colleges and universities to match faculty resources with student demand for classes, thereby improving efficiency [**74**].

Some start-up companies have taken this idea to the extreme. Instead of hiring employees, they make money by connecting people who want a service with people willing to provide that service. The **gig economy** refers to service workers who make a living by completing these types of short-term jobs for clients. These workers do not have a traditional employer, but typically rely upon one or more companies to connect them with clients. Uber, Lyft, Instacart, and Airbnb are well-

known examples of such companies. Uber and Lyft connect riders and drivers, Instacart is a grocery delivery service, and Airbnb connects people who need a place to stay with people who have accommodations for rent.

A 2021 survey revealed that 16 percent of US adults had earned money through the gig economy. The participation rate varied widely by race and ethnicity: 30 percent of Hispanic adults, 20 percent of Black adults, 19 percent of Asian adults, and 12 percent of white adults had earned money through a gig app. Two-thirds of current gig workers said that gig work was a side job and not their primary source of income [75].

)

Proponents of the gig economy say that it provides workers with independence and flexibility. Workers can make their own schedules and decide which assignments they want to accept. Critics say that people only take these jobs because they can't find stable employment. They point out that companies pit workers against each other in an effort to keep prices down. That's good for the people purchasing the services, but bad for the people providing the services. For example, Lyft and Uber engaged in a price war that resulted in significant reductions in the fares drivers earned [76].

“The big money goes to the corporations that own the software. The scraps go to the on-demand workers,” writes political economist Robert Reich [77]. “Uber drivers use their own cars, take out their own insurance, work as many hours as they want or can—and pay Uber a fat percentage. Worker safety? Social Security? Uber says it’s not the employer so it’s not responsible. Amazon’s Mechanical Turks work for pennies, literally. Minimum wage? Time-and-a-half for overtime? Amazon says it just connects buyers and sellers so it’s not responsible.”

Are gig workers employees or independent contractors? The answer is not clear because in some respects gig workers are more like employees, while in other respects they are more like independent contractors (Table 10.2). Some workers have concluded they would be better off as employees. Uber and Lyft drivers have filed lawsuits to be classified as employees rather than independent contractors [78]. If their lawsuit is successful, drivers could be entitled to an hourly wage and reimbursement for work-related expenses, such as gas and car insurance [79].

Table 10.2

Employee	*Driver for a Ride-sharing App*	*Independent Contractor*
Does not set own working hours	Sets own working hours	Sets own working hours
Work assigned by employer	Only feasible way to find customers is through app	Advertises to find work
Employer sets wages	Earnings set by app	Sets own fees for services
Entitled to minimum wage	Not entitled to minimum wage	Not entitled to minimum wage
Pays only employee's portion of Social Security taxes	Pays both employee's and employer's portions of Social Security taxes	Pays both employee's and employer's portion of Social Security taxes
Can get fired	Can be taken off list of providers	Cannot be fired
Eligible for unemployment insurance	Not eligible for unemployment insurance	Not eligible for unemployment insurance
Can unionize	Courts must determine	Cannot unionize

10.4.4 Monitoring

Information technology has given companies many new tools to monitor the activities of their employees. An American Management Association/ePolicy Institute survey in 2007 revealed that 66 percent of employers were monitoring the Internet use of their employees. Other examples of employee monitoring by American employers included video surveillance (48 percent), monitoring keyboard activity (45 percent), monitoring time spent on the phone (45 percent), and monitoring emails (43 percent) [80].

The principal purpose of monitoring is to identify inappropriate use of company resources [81]. A quarter of

companies in the United Kingdom have fired employees for improper use of the Internet. In the majority of these cases, the employee was surfing the Web for pornography. Another study of employee emails concluded that eliminating email containing gossip and jokes would cut the time staff spend reading email by 30 percent [82]. A study conducted by International Data Corporation concluded that between 30 and 40 percent of Internet use by employees was not work related [83].

Monitoring can help detect illegal activities of employees as well. By monitoring instant messaging conversations, employers have caught employees who had performed various misdeeds, including an employee who hacked into a company computer after being denied a promotion [84].

Monitoring is also used to ensure that customers are getting the products and services they need. Reviewing customer phone calls to help desks can reveal if the company ought to be providing its customers with better documentation or training [85].

Many companies use monitoring to gauge the productivity of their workers. For example, telemarketing firms keep track of how many calls their employees make per hour. Sometimes monitoring can help an organization assess the quality of the

work done by its employees. Major League Baseball used QuesTec's Umpire Information System to evaluate how well umpires were calling balls and strikes [86].

Companies are using wireless networks to track the locations of their employees. Knowing the location of service technicians enables an automated system to respond to a breakdown by alerting the technician closest to the malfunctioning piece of equipment. A system that tracks the locations of hospital physicians can upload a patient's file into the wireless laptop held by a doctor approaching a hospital bed.

More schools are using video cameras to increase security [87]. The school district in Biloxi, Mississippi, used gambling-generated tax receipts to install digital cameras in all 500 of its classrooms. An elementary school principal gushes, "It's like truth serum. When we have a he-said, she-said situation, 9 times out of 10, all we have to do is ask children if they want us to go back and look at the camera, and they fess up" [88].

It's an open question whether monitoring is ultimately beneficial to an organization. Obviously, organizations institute monitoring because they have reason to believe it will improve the quantity and/or quality of the work

performed by their employees. There is evidence that employee monitoring makes employees more focused on their tasks but also reduces job satisfaction [89].

10.4.5 Multinational Teams

In the 1980s, General Electric and Citibank set up software development teams in India. Since then, many corporations have established field offices in India, including Analog Devices, Cadence Design Systems, Cisco, Intel, Microsoft, and Sun Microsystems. Bangalore, in particular, has made an effort to become the Silicon Valley of India. Western-based companies use Indian companies to write software, process credit card applications, and do billing. Texas Instruments' chip design team in Bangalore has 200 patents to its name. Hewlett-Packard and Oracle both have thousands of employees in India. SAP has 500 engineers in Bangalore.

Multinational teams allow a company to have people at work more hours during the day. It becomes easier to have a call-support center open 24 hours a day. It is even possible for projects to be shuttled between multiple sites, allowing around-the-clock progress to be made on time-sensitive products. For example, a team in Palo Alto, California, can spend its day finding bugs in a piece of software, then hand

the bug reports over to a team in Bangalore that spends *its* day fixing the bugs [**90**].

However, India's main attraction to US companies is that they can pay employees in India much less than they pay employees in the United States. The total cost to a US company of employing a computer programmer in India is about $6,000–$9,000 a year. Companies say they need to lower their expenses in order to stay in business. If they go out of business, their US employees will lose their jobs. Hence creating multinational teams is a way for companies to stay in business and preserve jobs [**91**].

Creating multinational teams has disadvantages, too. The principal disadvantage is that the infrastructure in less-wealthy countries can make it more difficult to conduct business using the same universal method or system.

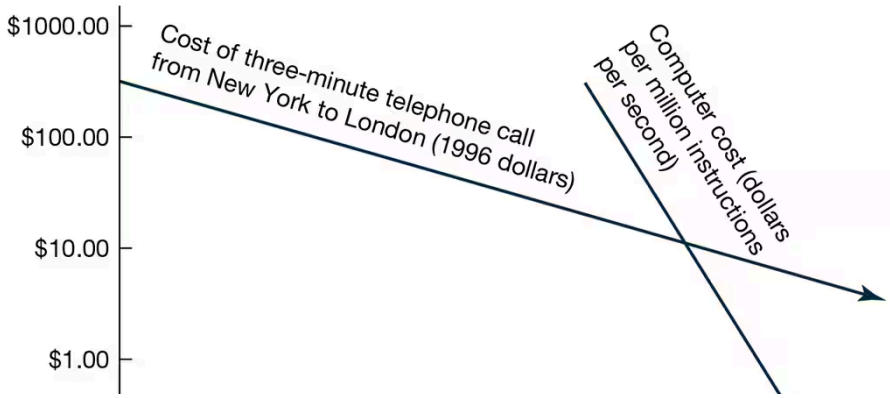
Despite the difficulties, corporations are increasingly making use of multinational teams. About 90,000 IT-related jobs in the United States are moving to foreign countries every year, and at American companies whose revenues are at least $5 billion, about a quarter of IT jobs have already moved offshore [**92**].

10.5 Globalization

Globalization refers to the process of creating a worldwide network of businesses and markets. Globalization results in greater mobility of goods, services, and capital around the world. Investments are made across national boundaries. Products manufactured in one country are sold in another. Consumers calling a telephone help center get connected with support technicians located on the other side of the world.

The rapidly decreasing cost of information technology made globalization possible (Figure 10.7). The cost of computing dropped by 99.99 percent between 1975 and 1995. The cost of an international telephone call from New York to London dropped by 99 percent between 1930 and 1996 [93]. Companies made extensive use of low-cost information technology to coordinate operations distributed around the planet.

Figure 10.7


$1000.00
$100.00
$10.00
$1.00
Cost of three-minute telephone call from New York to London (1996 dollars)
Computer cost (dollars per million instructions per second)

10.5.1 Arguments for Globalization

Those who favor globalization seek the removal of trade barriers between nations. The North American Free Trade Agreement (NAFTA) among Canada, the United States, and Mexico was a step toward globalization.

The World Trade Organization (WTO) is an international body that devises rules for international trade and promotes the goal of free trade among nations. The WTO and other proponents of globalization support free trade with these arguments:

1. *Free trade can increase everyone's standard of living.* Every country has a **comparative advantage** at producing certain products and services, meaning it can produce them at a lower opportunity cost than any other country. Consumers get better prices when each

area produces the goods or services it does best—corn in Kansas, automobiles in Ontario, semiconductors in Singapore, and so on—and then these products and services are bought and sold without trade barriers. When prices are lower, the real purchasing power of consumers is higher. Hence globalization increases everyone's standard of living.

2. *People everywhere benefit from paid work*. When they gain employment, their prosperity increases.

3. *Every example in the past century of a less-wealthy country becoming more prosperous has been the result of that country producing goods for the world market rather than striving for self-sufficiency* [**94**]. Contrast the economic success of South Korea with the situation of its neighbor North Korea.

4. *Creating jobs around the world reduces unrest and leads to more stability*. Countries with interdependent economies are less likely to go to war with each other.

10.5.2 Arguments Against Globalization

Ralph Nader, American trade unions, the European farm lobby, and organizations such as Friends of the Earth, Greenpeace, and Oxfam oppose globalization. They give these reasons why globalization is a bad trend:

1. *The United States and other governments should not be subordinate to the WTO*. The WTO makes the rules for globalization, but nobody elected it. It makes its decisions behind closed doors. Every member country, from the United States to the tiniest dictatorship, has one vote in the WTO.

2. *American workers should not be forced to compete with foreign workers who do not receive decent pay and working conditions*. The WTO does not require member countries to protect the rights of their workers. It has not banned child labor. Authoritarian regimes such as the People's Republic of China are allowed to participate in the WTO even though they do not let their workers organize into labor unions.

3. *Globalization has accelerated the movement of jobs out of the United States*.

4. *The removal of trade barriers hurts workers outside the United States, too*. For example, NAFTA removed

> tariffs among Canada, Mexico, and the United States. Because they receive agricultural subsidies from the US government, large American agribusinesses grow corn and wheat for less than its true cost of production and sell the grain in Mexico. Mexican farmers who cannot compete with these prices are driven out of business. Most of them cannot find jobs in Mexico and some end up emigrating to the United States [**95**].

Even if globalization is a good idea, there are reasons why a company may not choose to move its facilities to the place where labor is the least expensive. Interestingly, these arguments are more relevant to manufacturing jobs than they are to programming jobs. With automation, the cost of labor becomes a smaller percentage of the total cost of a product. Once the labor cost is reduced to a small enough fraction, it makes little difference whether the factory is located in China or the United States. Meanwhile, there are definite additional costs associated with factories outside the United States. If you include products in transit, non-US factories carry more inventory than identical factories in the United States. There are also more worries about security when the product is being made outside the United States. For these reasons, moving a factory to a less wealthy country is not always in the best interest of a company [**11**].

10.5.3 Dot-Com Bust Increased IT Sector Unemployment

In the 1990s, Intel's stock rose 3,900 percent, Microsoft's stock increased in value 7,500 percent, and Cisco Systems' stock soared an incredible 66,000 percent. That means $1,000 of Cisco stock purchased in 1990 was worth $661,000 at the end of 1999. Investors looking for new opportunities for high returns focused on **dot-coms**, Internet-related start-up companies. Speculators pushed up the values of many companies that had never earned a profit. Early in 2000, the total valuation of 370 Internet start-ups was $1.5 trillion, even though they had only $40 billion in sales (that's *sales*, not profits) [**96**].

In early 2000, the speculative bubble burst, and the prices of dot-com stocks fell rapidly. The ensuing "dot-com bust" resulted in 862 high-tech start-ups going out of business between January 2000 and June 2002. Across the United States, the high-tech industry shed half a million jobs [**97**]. In San Francisco and Silicon Valley, the dot-com bust resulted in

the loss of 13 percent of nonagricultural jobs, the worst downturn since the Great Depression [98].

10.5.4 People from Other Countries Working in the US IT Industry

Even while hundreds of thousands of information technology workers were losing their jobs, US companies hired tens of thousands of people from other countries to work in the United States. The US government grants these workers visas allowing them to work in the United States. The two most common visas are called the H-1B and the L-1.

An H-1B visa allows a visitor to work in the United States for up to six years. In order for a company to get an H-1B visa for an employee, the company must demonstrate that there are no US workers qualified to do the job. The company must also pay the new employee the prevailing wage for the job. Information technology companies have made extensive use of H-1B visas to bring in skilled workers from outside the United States and to hire international students graduating from US universities.

In the midst of the high-tech downturn, the US government continued to issue tens of thousands of H-1B visas: 163,600 in 2000–2001 and 79,100 in 2001–2002. Meanwhile, the unemployment rate among US citizens in the computer science profession was about 5.1 percent. Many of the 100,000 unemployed computer scientists complained to Congress about the large number of H-1B visas being issued. Some professional organizations argued against giving out any H-1B visas at all [**99**]. Congress decided to drop the H-1B quota to 65,000 for the fiscal year beginning October 1, 2003, and it initially set a quota of 65,000 for the following fiscal year. However, the 65,000 H-1B visas approved for 2004–2005 were filled in a single day; representatives of universities and technology companies said the quota was set too low [**100**]. Bill Gates said, "Anyone who's got the education and the experience, they're not out there unemployed" [**101**]. Congress responded in May 2005 by allowing an exemption for an additional 20,000 visas for people with advanced degrees (master's or higher).

The annual quota of 65,000 H-1B visas and the exemption for an additional 20,000 visas for people with advanced degrees remain in effect. When the economy is strong, the demand for H-1B visas greatly exceeds the number of visas available, and the federal government holds a lottery to

determine which petitions will move forward. Every year the US government holds a lottery for H-1B visas because the number of applicants greatly exceeds the number of visas available.

The other important work visa is called the L-1. American companies use L-1 visas to move workers from overseas facilities to the United States for up to seven years. For example, Intel employees in Bangalore, India, could be transferred to Hillsboro, Oregon, if they held an L-1 visa. Employees brought in to the United States under an L-1 visa do not need to be paid the prevailing wage. That saves employers money.

Critics of L-1 visas claim lower-paid workers from other countries are replacing higher-paid US workers within the walls of high-tech facilities located in the United States. The US Congress has put no limit on the number of L-1 visas that may be issued in any given year, but the number of people working in the United States under L-1 visas is much smaller than the number holding H-1B visas. In 2017 about 78,000 people were employed in the United States under the L-1 visa program [**102**].

10.5.5 International Competition

The debate over the number of visas to grant people seeking employment in the United States should not mask another trend: the increasing capabilities of IT companies within other nations, particularly China and India.

In 1990 China's computer hardware industry was virtually nonexistent. IBM agreed to sell its PC division to Chinese computer manufacturer Lenovo for $1.75 billion in 2004, making Lenovo the number-three manufacturer of PCs in the world [**103**]. That was the year China became the world's leading producer of personal computer hardware. Today, 90 percent of all personal computers are manufactured in China [**104**].

India's outsourcing industry is large; Indian companies now employ more than a million people and have annual sales exceeding $60 billion. About two-thirds of these sales are in outsourcing IT work, such as designing, programming, and maintaining computer software. The other third are in outsourcing business processes, such as call centers, medical transcription, and X-ray interpretation [**105**].

Some Chinese universities are becoming recognized for their research expertise. For example, the Institute of Computing Technology at the Chinese Academy of Science and Tsinghua University have been actively involved in the development of the Open64 optimizing compiler [**106**].

More evidence of global competition comes from the annual International Collegiate Programming Contest. When the contest began in 1977, only schools from North America and Europe competed. Today, it is a truly international competition, dominated by teams from Russia and China. When a team from the Massachusetts Institute of Technology won the competition in 2022, that was the first win by a US team in 25 years.

10.5.6 Electronic Waste

Electronic waste (**e-waste**) refers to discarded electronic equipment. Because of globalization, managing electronic waste has become a worldwide problem. More than 50 million metric tons of e-waste are generated every year. That works out to about 14 pounds of e-waste per human per year. The generation of e-waste is expected to increase by 33 percent in the next decade [**107**].

A variety of factors are leading to the rapid increase in the generation of e-waste:

- Rising incomes in many countries have increased consumer demand for electronic devices. When more people purchase new devices, there are more people to dispose of old devices.
- The COVID-19 pandemic forced millions of people to work and study from home, leading to a surge in purchases of electronic equipment.
- Shorter product cycles encourage consumers to replace devices more frequently. For example, many smartphone manufacturers release new models every year, tempting consumers to switch to new models with a few new features. Batteries on portable devices deteriorate over time, but many devices are designed to make batteries difficult to replace, encouraging consumers to upgrade their devices rather than pay for expensive repairs.

Residents of the United States are provided a variety of e-waste recycling options, based on which state they live in. These options include curbside recycling, collection events, and designated collection sites. Still, less than 10 percent of

the e-waste generated every year in the United States is properly collected and recycled [**107**]. Put another way, more than 90 percent of e-waste in the United States is improperly disposed of. E-waste contains lead, mercury, cadmium, and chromium. When e-waste is thrown out with garbage that is taken to a landfill, these toxic substances can leach into the soil and groundwater. In addition, e-waste contains gold, silver, palladium, copper, and aluminum. When e-waste is sent to a landfill, these valuable metals cannot be recovered and reused.

Per capital e-waste generation in the European Union is the highest in the world. However, 43 percent of e-waste in the European Union is collected and recycled, a much better rate than in the United States [**107**].

Millions of tons of e-waste are exported each year from wealthier countries to countries where e-waste processing is not tightly regulated by the government. The United States exports 43–52 container loads of e-waste to other countries every day. Traditional hubs for recycling e-waste include India, China, Ghana, Indonesia, Nigeria, the Philippines, Thailand, and Vietnam [**107**].

In countries receiving e-waste, most e-waste recovery is performed outside formal recycling plants using “improper

and unsafe techniques" [**107**]. India is now the top destination of e-waste from other countries. New Delhi is the center of the e-waste processing industry in India, and unregulated e-waste recyclers have created a serious air pollution problem in that city [**107**].

Another well-known example of unregulated e-waste recycling is Guiyu, China. At one time Guiyu was the largest e-waste processing site in the world. About 60,000 workers at thousands of workshops processed about 1.5 million tons of e-waste every year, grinding plastic cases into bits and putting circuit boards into kilns or acid baths to extract lead, silver, and other metals [**108**]. Water from local wells was not safe to drink [**109**]. Tests revealed that 80 percent of the children in Guiyu had dangerously high levels of lead in their blood [**110**]. In 2021 China banned the importation of e-waste from other countries. A follow-up study revealed that after the ban took effect, local air pollution at China's e-waste disposal hubs was reduced by 15–28 percent [**111**].

Improper recycling of e-waste results in significant harm to the environment and to human health in less wealthy countries. There is an urgent need to construct more facilities that can safely and cost-effectively process e-waste [**107**].

There is also a need to significantly improve the amount of e-waste that is recycled, particularly in the United States.

10.6 The Digital Divide

The **digital divide** refers to the situation in which some people have access to modern information technology while others do not. The underlying assumption motivating the term is that people who use cell phones, computers, and the Internet have opportunities denied to people without access to these devices. The idea of a digital divide became popular in the mid-1990s with the rapid growth in popularity of the World Wide Web.

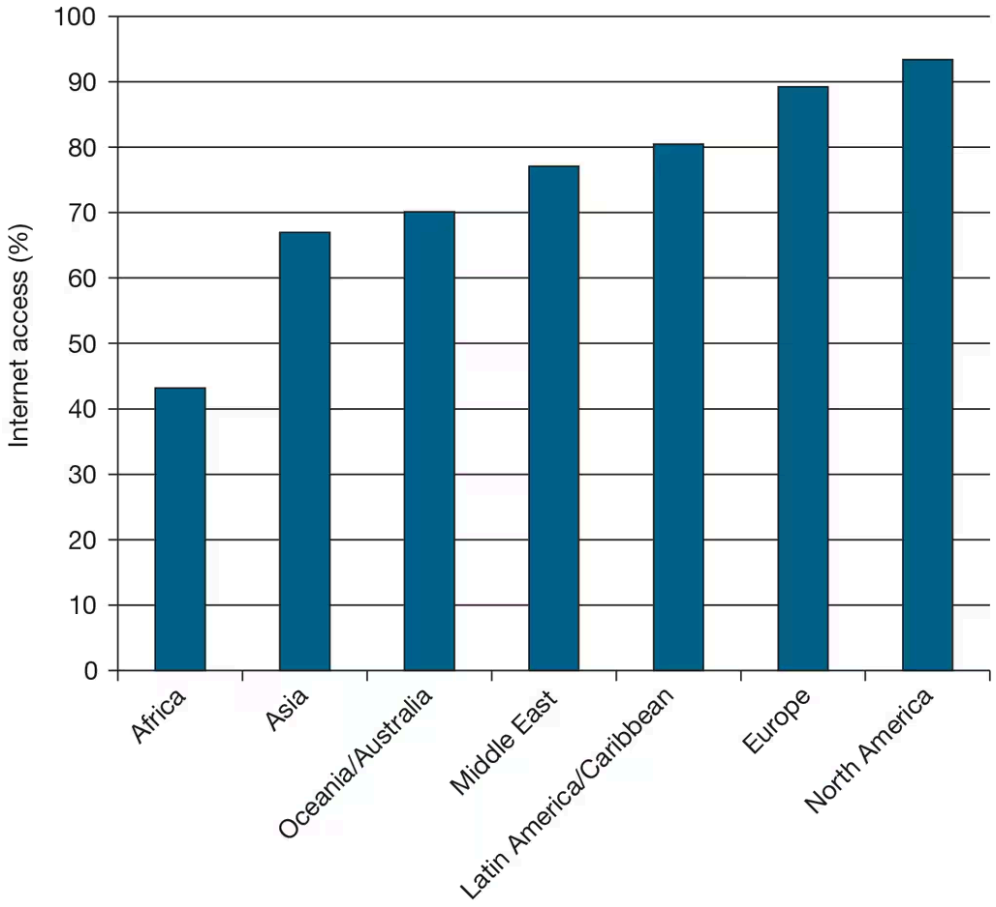
According to Pippa Norris, the digital divide has two fundamentally different dimensions. The **global divide** refers to the disparity in Internet access between more industrialized and less industrialized nations. The **social divide** refers to the difference in access based on income within a particular country [**112**].

10.6.1 Global Divide

There is plenty of evidence of what Norris calls the global divide. One piece of evidence is the percentage of people with

Internet access (Figure 10.8). In 2023 about 5.4 billion people, representing roughly 68 percent of the world's population, had access to the Internet. Access to the Internet in North America and Europe was significantly above this average, while access in Africa was well below [**113**].

Figure 10.8



Percentage of people with Internet access, by world region.

What is hampering Internet development in less technologically developed countries?

1. *Often there is little wealth*.

In many of these countries there is not enough money to provide everyone in the country with the necessities of life, much less pay for Internet connections.

2. *Many of these countries have an inadequate telecommunications infrastructure*.

   For example, less than 30 percent of the people in North Korea, Eritrea, and the Central African Republic have cell phones [**114**]. Many poor people have no access to newspapers, radio, or television [**112**].

3. *The primary language is not English*.

   English is the dominant language for business and scientific development, giving English-speaking countries a comparative advantage with respect to competing in the global marketplace.

4. *Literacy is low and education is inadequate*.

   Half the population in less-wealthy countries has no opportunity to attend secondary schools. There is a strong correlation between literacy and wealth, both for individuals and for societies [**64**].

5. *The country's culture may not make participating in the Information Age a priority* [**115**].

10.6.2 Social Divide

Even within wealthy countries such as the United States, the extent to which people use the Internet varies significantly according to age, wealth, and educational achievement. Pew Internet polled Americans to find out how many made use of the Internet as of early 2021. Online access varied from 99 percent of 18- to 29-year-olds to 75 percent of those 65 and over. Fully 99 percent of adults living in households with annual incomes of at least $75,000 used the Internet, compared to 86 percent of adults living in households with annual incomes less than $30,000. While 98 percent of those with a college degree used the Internet, only 86 percent of those who dropped out of high school went online. The report also noted that the less-connected groups are gradually catching up with the more-connected groups [**116**].

10.6.3 Models of Technological Diffusion

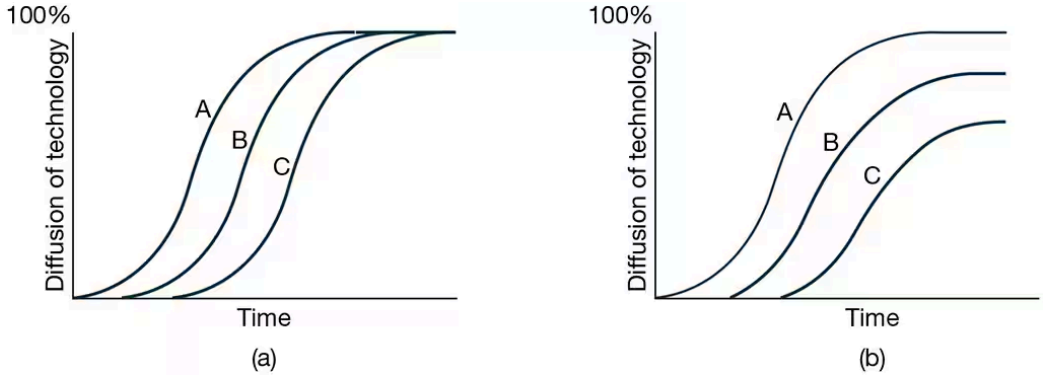
New technologies are usually expensive. Hence the first people to adopt new technologies are those who are better off. As the technology matures, its price drops dramatically, enabling more people to acquire it. Eventually, the price of the technology gets low enough that it becomes available to nearly everyone.

The history of the consumer VCR illustrates this phenomenon. The first VHS VCR, introduced by RCA in 1977, retailed for $1,000 ($3,562 in 2009 dollars). In 2009 you could buy a VHS VCR from a mass-marketer for under $30. That means between 1977 and 2009, the price of a VCR in constant dollars fell by more than 99 percent! As the price declined, more people could afford to purchase a VCR and sales increased rapidly. The VCR progressed from a luxury that only the rich could afford to a consumer product found in nearly every American household.

Technological diffusion refers to the rate at which a new technology is assimilated into a society. Two different theories predict how a new technology is acquired by people in a society, based on their socioeconomic status (Figure 10.9). We divide society into three groups. People with the highest socioeconomic status are in group A, people with the

lowest socioeconomic status are in group C, and group B consists of those people in the middle.

Figure 10.9



Two models for technological diffusion. In both models the most advantaged group A is the first to adopt a new technology, while the least advantaged group C is the last to adopt it. (a) In the normalization model, the technology is eventually embraced by nearly everyone in all groups. (b) In the stratification model, the eventual adoption rate of the technology is lower for less advantaged groups.

In the **normalization model** (Figure 10.9a), group A begins to adopt the technology first, followed by group B, and finally group C. However, at some point nearly everyone in all three groups is using the new technology.

In the **stratification model** (Figure 10.9b), the order of adoption is the same as in the normalization model. However, in this model the eventual number of people in group C who adopt the technology is lower than the number of adopters in group A. The percentage of people in group B who adopt the technology is somewhere between the levels of the other two groups.

Technological optimists believe the global adoption of information technology will follow the normalization model. Information technology will make the world a better place by reducing poverty in less wealthy countries.

Technological pessimists believe information technology adoption will follow the stratification model, leading to a permanent condition of "haves" and "have-nots." Information technology will only exacerbate existing inequalities between rich and poor nations and between rich and poor people within each nation [**112**].

10.6.4 Critiques of the Digital Divide

Mark Warschauer has suggested three reasons why the term "digital divide" is not helpful. First, it tends to promote the idea that the difference between the "haves" and the "have-nots" is simply a question of access. Some politicians have jumped to the conclusion that providing technology will close the divide. Warschauer says this approach will not work. To back his claim, he gives as an example the story of a small town in Ireland.

While many factories in Ireland produced IT products, there was not a lot of IT use among Irish citizens. Ireland's telecommunications company held a contest in 1997 to select and fund an "Information Age Town." The winner was Ennis, a town of 15,000 in western Ireland. The $22 million in prize money represented $1,200 per resident, a large sum for a community with low income and a high level of unemployment. Every business was equipped with an Integrated Services Digital Network (ISDN) line, a Web site, and a smart card reader. Every family received a smart card and a personal computer.

Three years later, there was little evidence of people using the new technology. Devices had been introduced without adequately explaining to the people why they might want to use them. The benefits were not obvious. Sometimes the technology competed with social systems that were working just fine. For example, before the introduction of the new technology, people without jobs visited the local social services office three times a week to sign in and get an income support payment. These visits served an important social function. They gave people an opportunity to visit with others and keep their spirits up. Once the PCs were introduced, they were supposed to "sign in" and receive their payments over the Internet. Many of them did not like the

new system. It appears that many of the PCs were illegally sold. The people without jobs simply went back to reporting in person to the office.

For IT to make a difference, social systems must change as well. The introduction of information technology must take into account local culture, which includes language, literacy, and community values.

Warschauer's second criticism of the term "digital divide" is that it implies everyone is on one side or another of a huge canyon. Everybody is put into one of two categories: "haves" and "have-nots." In reality access is a continuum, and each individual occupies a particular place on it. For example, how do you categorize someone who has a slow Internet connection? Certainly, that person has online access, but they are not able to retrieve the same wealth of material as someone with a broadband connection.

Third, Warschauer says that the term "digital divide" implies that a lack of access will lead to a less advantaged position in society. Is that the proper causality? Models of technological diffusion show that those with a less-advantaged position in society tend to adopt new technologies at a later time, which is an argument that the causality goes the other way. In

reality, there is no simple causality. Each factor affects the other [64].

Rob Kling has put it this way:

> [The] big problem with "the digital divide" framing is that it tends to connote "digital solutions," i.e., computers and telecommunications, without engaging the important set of complementary resources and complex interventions to support social inclusion, of which informational technology applications may be enabling elements, but are certainly insufficient when simply added to the status quo mix of resources and relationships. [64, pp. 7–8]

Finally, Warschauer points out that the Internet does not represent the pinnacle of information technology. In the next few decades, dramatic new technologies will be created. We will see these new technologies being adopted at different speeds, too.

10.6.5 Online Courses

The Community College Research Center conducted a study of online education at two statewide community systems, one

in the southern United States and the other in the western United States. Their study revealed that students who take online courses are less likely to complete and perform well in them, compared with students who take the same courses in a traditional classroom setting. The study also showed that the online experience widened the achievement gap between white and Black students and between those with higher GPAs and those with lower GPAs [**117**].

The Community College Research Center study provides evidence that a shift toward online education could exacerbate differences in success rates that already exist between different subgroups of students. It reinforces Warschauer's point that the difference between the "haves" and the "have-nots" in society is not simply a question of access to a technology or even information.

10.6.6 Net Neutrality

In the 1990s, corporations that operate the long-distance Internet backbone connections in the United States suggested that they might begin **tiered service**—charging more for higher-priority routing of Internet packets. These companies said that tiered service would be needed in the future to guarantee a satisfactory level of service to companies that

require it, such as voice over Internet protocol (VoIP) providers [**118**].

Content providers such as Google and Yahoo joined forces with the American Library Association and consumer groups to oppose any notion of tiered service. These groups asked the US Congress to enact "net neutrality" legislation that would require Internet service providers to treat all packets the same. Consumer groups suggested that if tiered service were enacted, only large corporations would be able to pay for the highest level of service. Small start-up companies wouldn't be able to compete with established corporate giants. Hence tiered service would discourage innovation and competition. Another argument against tiered service was based on the concern that companies controlling the Internet might block or degrade access to nonfavored content or applications [**118**]. For example, a customer with an AT&T/Yahoo DSL connection might find that high-definition video content from AT&T channels performs better than high-definition video from other providers [**119**]. Net neutrality advocates said this would be unfair and should be prevented, pointing out that 95 percent of consumers have only two choices for broadband access: the local cable company or the local telephone company [**120**].

Opponents of net neutrality legislation suggested that allowing people to pay more to get a higher quality of service can benefit consumers. For example, rapid delivery of data packets would be more valuable to a person using the Internet for videoconferencing than a person who simply sends email messages. Internet backbone providers argued that even though there was currently enough bandwidth, the rapidly increasing popularity of YouTube and other online video sites would soon fill the Internet's data pipes. A significant amount of money would be needed to upgrade the Internet infrastructure to support the higher-bandwidth applications of the future. This money ought to come from the companies like Netflix that sell access to data-intensive content [**118**].

In February 2015, during the administration of President Barack Obama, the Federal Communications Commission issued the Open Internet Order to preserve net neutrality. It prohibited telecommunications companies from engaging in three activities: blocking content, throttling back the speed of transmissions, and providing a higher speed of service to people or businesses that pay more [**121**]. FCC Chairman Tom Wheeler said, "No one—whether government or corporate—should control free, open access to the Internet" [**122**]. The FCC grounded its authority to make these rules

on Title II of the Telecommunications Act, in effect deciding that the Internet should be regulated as a public utility.

The FCC's decision was immediately hailed by some groups and criticized by others. Netflix issued a statement saying, "The net neutrality debate is about who picks winners and losers online: Internet service providers or consumers. Today the FCC settled it: Consumers win" [**123**]. Meanwhile, Broadband for America, an advocacy group that has Internet service providers among its members, issued a statement saying, "The FCC's decision to impose obsolete telephone-era regulations on the high-speed Internet is one giant step backwards for America's broadband networks and everyone who depends upon them. These 'Title II' rules go far beyond protecting the Open Internet, launching a costly and destructive era of government micromanagement that will discourage private investment in new networks and slow down the breakneck innovation that is the soul of the Internet today" [**124**].

Under the administration of President Donald Trump, the FCC changed course, and in December 2017 the commissioners voted to repeal the net neutrality rules put in place by the Obama administration. The repeal took effect in June 2018 [**125**]. Responding to the FCC's decision,

lawmakers in dozens of states introduced legislation to preserve net neutrality rules. In March 2018 the state of Washington became the first state to preserve for its residents the net neutrality rules established by the FCC in 2015 [**126**].

In 2018 India adopted strong net neutrality rules. The regulations state that "Internet access services should be governed by a principle that restricts any form of discrimination or interference in the treatment of content" [**127**]. The European Union passed a net neutrality law in 2015, but critics said its many loopholes severely weakened the legislation [**128**]. Brazil, Canada, Israel, Japan, Mexico, Russia, Slovenia, South Korea, and Switzerland have also passed net neutrality laws [**129**].

10.7 The “Winner-Take-All” Society

The Declaration of Independence states that “all men are created equal,” but we live in a society in which some people have far more wealth and power than others. What if everyone were guaranteed roughly the same amount of income? The traditional answer to this question is that there would be little motivation for people to exert themselves, either mentally or physically. If everyone were paid the same, there would be no point in getting an education, taking risks, or working hard. Productivity would be low, and the overall standard of living would be poor. For this reason, many people believe a superior alternative is a market economy that rewards innovation, hard work, and risk taking by compensating people according to the value of the goods they produce.

In *The Winner-Take-All Society*, economists Robert Frank and Philip Cook explore the growth of markets in which a few top performers receive a disproportionate share of the

rewards. Their book is the primary source for this section [130].

Frank and Cook observe that the winner-take-all phenomenon has existed for quite a while in the realms of sports, entertainment, and the arts. A few "superstar" athletes, actors, and novelists earn millions from their work and garner lucrative endorsements, while those who perform at a slightly lower level make far less. However, the winner-take-all phenomenon has now spread throughout our global economy. Sometimes the qualitative difference between the top product and the second-best product is very slight, yet that can be the difference between success and failure. Hence corporations compete for the top executive talent that can give them the edge over their competition. The compensation of CEOs at America's largest corporations has risen much faster than the wages of production workers (Figure 10.10) [131].

Figure 10.10

Several factors have influenced the winner-take-all phenomenon in our economy:

1. *Information technology and efficient transportation systems make it easier for a leading product to dominate the worldwide market.*

   For example, consider a music studio that has a digital recording of the world's best orchestra playing Beethoven's Symphony No. 5 in C Minor. The studio can produce millions of perfect copies of this recording, enough for every classical music lover on the planet. Why would anyone want to listen to the second-best orchestra when a CD of the best orchestra is available for virtually the same price?

2. *Network economies encourage people to flock to the same product.*

   If by chance you should need to use someone else's computer, it is far more likely that person will own a Windows PC than a Macintosh. In this respect, knowing how to use a Windows computer has greater

utility than knowing how to use a Macintosh. If a person cannot decide which computer to purchase, this factor alone may encourage someone to buy a Windows PC.

3. *English has become the de facto language of international business*.

   English is the native language in 12 countries, including the United States, which is the dominant economic power on the planet. Another 56 countries teach English in their schools. The dominance of English makes it easier for products to find a worldwide market.

4. *Business norms have changed*.

   In the past large businesses promoted from within and would not recruit executives from other firms. Today firms vigorously compete with each other for top executive talent.

10.7.1 Harmful Effects of Winner-Take-All

Frank and Cook argue that winner-take-all effects are bad for the economy for a variety of reasons. First, winner-take-all markets increase the gap between people who are most and least wealthy. Between 1979 and 2019, the inflation-adjusted incomes of the top 1 percent of US wage earners increased by 190 percent, while the inflation-adjusted incomes of those in the bottom 90 percent increased by only 26 percent.

Winner- take-all effects draw some of the most talented people into socially unproductive work. The problem with winner-take-all contests is that they attract too many contestants. For every comedian who hosts a late-night talk show, tens of thousands of comedians struggle in nightclubs, hoping for their big break. The multimillion-dollar incomes of a relatively few high-profile attorneys help attract many of the brightest college students toward law school. We end up with a glut of lawyers. Meanwhile, there is a shortage of nurses and nuclear engineers.

Winner- take-all markets create wasteful investment and consumption. For example, universities compete to attract students. When a university spends money to create an amenity like an improved recreation center, that can give it an advantage over its competition. However, when the competing universities also spend money and improve their

recreation centers, the advantage is lost. All of the universities have spent a lot of money, and none of them have gained an advantage.

A disproportionate share of the best and brightest college students become concentrated in a few elite institutions. “The day has already arrived,” write Frank and Cook, “when failure to have an elite undergraduate degree closes certain doors completely, no matter what other stellar credentials a student might possess” [**130**, p. 11]. Many Wall Street firms will not even interview candidates who did not graduate from one of a very small number of top law schools. These law schools show a preference for graduates of elite undergraduate programs. Hence high school students interested in reaching the top of the legal profession know their best chance is to do their undergraduate work at an elite school. The result is a tremendous competition for a relatively small number of openings at these colleges, while in truth there are hundreds of top-quality public and private colleges and universities in the United States.

Winner- take-all is not fair because it gives much greater rewards to the top performers than those whose performance is only slightly inferior. Here is an example from the world of professional sports, where winnings and performance data

are objective and publicly available. Scottie Scheffler, Sahith Theegala, and Sung Kang all play on golf's PGA Tour. Their skill levels are very close (see Table 10.3), but their earnings varied dramatically during the 2021–22 season. Scottie Scheffler earned an average of $561,876 for every tournament he entered, versus $97,646 for Sahith Theegala and only $11,593 for Sung Kang.

Table 10.3

Metric	*Scottie Scheffler*	*Sahith Theegala*	*Sung Kang*
Driving distance (yards)	312	304	294
Driving accuracy (%)	60	54	61
Greens in regulation (%)	72	66	66
Putts per green in regulation	1.72	1.76	1.77
Winnings per tournament	$561,876	$97,646	$11,593

Comparison of personal statistics of PGA Tour professionals Scottie Scheffler, Sahith Theegala, and Sung Kang for the 2021-22 season.

Winner- take-all markets harm our culture. Here's why. People are social; they like to read the same books and see the same movies as their friends. It gives them something to talk about. Suppose two books have about the same appeal to a consumer, but one of them is on a best-seller list. The consumer is more likely to select the book on the best-seller list, because it increases the probability they will encounter a friend who has read it. But that means it's really important for a book publisher to get its books on the best-seller list. Publishers know that books written by "name" authors have

a greater chance of making the best-seller list than books written by new authors. This knowledge can lead a publisher to give a big advance to a well-known author to produce a second-rate work, rather than invest the same resources in developing an unknown, but more talented, author. The same effect happens with movie producers. Hoping for the largest possible sales on the first weekend, they bankroll second-rate sequels to big hits rather than original stories filmed by lesser-known directors.

;

10.7.2 Reducing Winner-Take-All Effects

If winner-take-all markets have harmful consequences on our economy and society, what can be done? Frank and Cook suggest four ways to reduce winner-take-all effects. First, societies can enact laws limiting the number of hours that stores remain open for business. These laws ensure parity among competing businesses and prevent them from engaging in positional arms races. Without these laws, one business may extend its hours in order to gain an advantage over its competitors. Soon all of its competitors follow suit. Parity is restored, but now all the employees must bear the

burden of the longer hours. Regulations on business hours are often called “blue laws.”

Second, in the absence of laws, businesses can form cooperative agreements to reduce positional arms races. An example is when a group of professional sports team owners agrees to establish a cap on team salaries.

Third, more progressive tax structures reduce excess competition for the few handsomely rewarded positions. Back in 1961, the marginal tax rate on income in the highest US tax bracket was 91 percent. By 1989, the highest marginal income tax rate had been lowered to 28 percent. (By 2023, it had risen back to 37 percent.) Consumption taxes and luxury taxes are other ways of targeting the wealthiest people. Heavily taxing those with the highest incomes makes a higher income less attractive and dissuades some people from competing for the highest-paying jobs. Society benefits when these people engage in more productive work.

Finally, campaign finance reform can reduce the political power of the wealthiest 1 percent of the population, who control more than one-third of the wealth. Reducing the political power of the very wealthy is another way to reduce the attraction of competing for the highest-paying positions.

Summary

This chapter has explored a variety of ways in which automation and globalization have affected the workplace. We began by asking the question, does automation increase unemployment? On the surface, the answer to this question seems obvious: of course automation increases unemployment. That is what automation means—replacing human labor with machine labor. Industrial robots, voice-mail systems, and a myriad of other devices have displaced millions of workers over the past 50 years. However, a deeper look reveals how automation can create jobs, too. When products are less expensive, more people want to buy them, increasing the number that must be made. If products are less expensive, consumers have more money left to spend, which increases demand for other products. Finally, some people are involved in creating and maintaining the machines themselves. For these reasons, the rapid introduction of automation has not yet led to widespread unemployment in the countries where automation is used the most.

Thanks to automation, productivity has more than doubled since World War II. However, the length of the workweek in the most highly industrialized nations has not decreased by half. Instead, productivity has been used to increase the standard of living. This choice is understandable since many contemporary societies define success in terms of wealth and material possessions. However, not all cultures have the same values. People in some "primitive" cultures choose to work much shorter hours.

Recent breakthroughs in artificial intelligence, particularly generative AI systems such as ChatGPT, lead many, though not all, experts to believe that artificial general intelligence is on the horizon. Dozens of corporations, professional organizations, and government agencies have issued guidelines for AI development in the hope that people will be able to trust the actions of future AI systems. There is broad agreement regarding the basic principles of transparency, fairness, privacy, reliability, and accountability, but many questions remain unanswered. In particular, how will these principles be operationalized?

Information technology has transformed the way businesses organize themselves. Rapid and inexpensive communications allow many more information channels to open up within

organizations, which can speed up processes and eliminate middlemen. Evidence of more flexible organizational structures includes the rise of telework and multinational teams. Improvements in information technology have also given management unprecedented access to the moment-by-moment activities of employees. Workplace monitoring has become the rule rather than the exception in large corporations. Information technology made possible a rapid transition to remote work during the COVID-19 pandemic and a substantial amount of people maintaining a hybrid work schedule after the pandemic.

As modern information technology has spread around the world, corporations form tightly connected networks and sell their products and services in many markets. This process is called globalization. Advocates of globalization claim it creates jobs for people in poorer countries and increases competition, resulting in lower prices and a higher standard of living for everyone. Critics of globalization say it forces workers in wealthier countries to compete with people willing to work for a fraction of the pay.

The notion that only manufacturing jobs could be lost to overseas competition was disproved by historical events. While the dot-com bus put hundreds of thousands of US IT

professionals out of work, US companies offshored hundreds of thousands of jobs to India and some other countries in Asia where well-educated people receive salaries that are a fraction of what a US employee receives. High-tech workers in the United States who are out of work have criticized companies for hiring large numbers of people to come and work in the United States under H-1B or L-1 visas. Companies respond that reducing labor costs is a necessity in a competitive marketplace. In order to survive and thrive, companies must keep costs down and profits up.

The "digital divide" is a way of splitting people into two groups: those who have access to information technology and those who do not. The term is based on the premise that access to information technology is a prerequisite for success in the Information Age. Some also assume that simply giving people access to the technology solves the problem. Pippa Norris points out that there are several fundamentally different dimensions to the digital divide. One dimension separates the more industrialized nations from the less industrialized nations. Another dimension separates rich and poor within a particular country. Mark Warschauer says the notion of a digital divide is too simplistic for three reasons. First, people have widely varying access to information technology. Access should be seen as a continuum, not a

division into “haves” and “have-nots.” Second, simply giving people information technology devices, such as computers, cell phones, and Internet accounts, does not guarantee they will take full advantage of the opportunities those devices provide. For IT to make a difference, social systems must be taken into account. According to Warschauer, the use of information technology “is a social practice, involving access to physical artifacts, content, skills, and social support” [**64**, p. 46]. Third, it’s too simplistic to say that a lack of access causes someone to have lower socioeconomic status. You could just as easily say that people with lower socioeconomic status adopt new technologies later. In reality, each factor influences the other.

Frank and Cook invented the term “winner-take-all society” to refer to the way that information technology, the spread of English, network effects, and other factors are creating marketplaces where a few top performers gain a disproportionate share of the rewards. They present evidence that winner-take-all effects harm our economy and our culture, and they suggest actions that can be taken to reduce the winner-take-all phenomenon.

Further Reading, Listening, and Viewing

Rachel Botsman. “The Currency of the New Economy Is Trust.” TED Talk, September 2012. 19:42. www.ted.com/talks/.

Peter Coy. “Work Is Intrinsically Good. Or Maybe It’s Not?” *New York Times*, September 5, 2022. https://www.nytimes.com/2022/09/05/opinion/work-labor-morality.html

Ashok Goel. “A Teaching Assistant Named Jill Watson.” TEDxSanFrancisco, October 6, 2016. 19:17. www.youtube.com/watch?time_continue=1153&v=WbCguICyfTA.

CGP Grey. “Humans Need Not Apply.” YouTube, August 13, 2014. 15:00. www.youtube.com/watch?v=7Pq-S557XQU.

Will Douglas Heaven. “Artificial General Intelligence: Are We Close, and Does It Even Make Sense to Try?” *MIT Technology Review*, October 15, 2020. https://www.technologyreview.com/2020/10/15/1010461/artifi

general- intelligence-robots-ai-agi-deepmind-google-openai/

Tiffany Hsu. “What Can You Do When A.I. Lies About You?” *New York Times*, August 7, 2023. https://www.nytimes.com/2023/08/03/business/media/ai-defamation-lies-accuracy.html

Jodi Kantor and Arya Sundaram. “The Rise of the Worker Productivity Score.” *New York Times*, August 14, 2022. https://www.nytimes.com/interactive/2022/08/14/business/worl productivity-tracking.html

Alexander C. Karp. “Our Oppenheimer Moment: The Creation of A.I. Weapons.” *New York Times*, July 25, 2023. https://www.nytimes.com/2023/07/25/opinion/karp-palantir-artificial-intelligence.html

Kevin Kelly. “Better Than Human: Why Robots Will—and Must—Take Our Jobs.” *WIRED*, December 24, 2012. www.wired.com.

Yul Kwon. “Made in the USA.” *America Revisited*, May 2, 2012. 53:10. video.pbs.org.

Gary Marcus and Ernest Davis. *Rebooting AI: Artificial Intelligence We Can Trust*. Pantheon Books, New York, 2019.

Cade Metz. "'The Godfather of A.I.' Leaves Google and Warns of Danger Ahead." *New York Times*, May 1, 2023. https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html

Kevin Roose. "We Need to Talk About How Good A.I. Is Getting." *New York Times*, August 24, 2022. https://www.nytimes.com/2022/08/24/technology/ai-technology-progress.html

Tom Simonite. "The WIRED Guide to Artificial Intelligence." *WIRED*, February 7, 2023. https://www.wired.com/story/guide-artificial-intelligence/?utm_brand=wired&utm_mailing=WIR_SubPersRec_1_020120

Natasha Singer. "At This School, Computer Science Class Now Includes Critiquing Chatbots." *New York Times*, February 6, 2023. https://www.nytimes.com/2023/02/06/technology/chatgpt-schools-teachers-ai-ethics.html

Daniel Suarez. “The Kill Decision Shouldn’t Belong to a Robot.” TED Talk, June 2013. 13:20. www.ted.com/talks/.

Stuart A. Thompson and Tiffany Hsu. “How Easy Is It to Fool A.I.-Detection Tools?” *New York Times*, June 28, 2023. https://www.nytimes.com/interactive/2023/06/28/technology/ai detection-midjourney-stable-diffusion-dalle.html

Nitasha Tiku. “The Google Engineer Who Thinks the Company’s AI Has Come to Life.” *Washington Post*, June 11, 2022. https://www.washingtonpost.com/technology/2022/06/11/goog ai-lamda-blake-lemoine/

Review Questions

1. What are some benefits brought about by automation? What are some harms brought about by automation?
2. What evidence has been given to show that automation eliminates jobs? What evidence has been given to show that automation creates more jobs than it destroys?
3. If automation has doubled productivity since World War II, why hasn't the workweek gotten shorter?
4. Define "artificial intelligence" in your own words.
5. Why did the approach to AI that depended on programming high-level human reasoning skills give way to neural network models?
6. What is the difference between "artificial intelligence" and "artificial general intelligence"?
7. What is a digital watermark? How do digital watermarks relate to discussions of artificial intelligence?

8. In what ways has information technology led to changes in the structure of an organization?

9. Briefly describe some benefits and harms associated with remote work.

10. Proponents of globalization claim that it helps workers in less-wealthy countries. Opponents of globalization claim the opposite. Summarize the evidence pro and con.

11. Provide a few pieces of evidence demonstrating that access to modern information technology is not uniform.

12. What is the assumption underlying the term “digital divide”? Provide a few arguments that have been raised to cast doubts about the soundness of this assumption.

13. Provide an example of the “winner-take-all” effect, without repeating an example already appearing in the book.

Discussion Questions

14. Voltaire wrote, “Work keeps at bay three great evils: boredom, vice, and need.” Do you agree?

15. Would you accept a salaried position (paying a fixed amount each month rather than paying by the hour) if you knew it would require you to work at least 50 hours per week in order to complete the required work?

16. German automaker Daimler has instituted a policy allowing employees going on vacation to select an “out of office” option for their email account that deletes all incoming messages while they are away. Those sending an email to vacationing employees receive a message informing them that their message has not been received and inviting them to contact someone else identified by the vacationer. Daimler board member Wilfried Porth says, “Our employees should relax on holiday and not read work-related emails. With ‘Mail

on Holiday' they start back after the holidays with a clean desk" [**132**]. Would you like to see all companies establish a similar policy?

17. If automation leads to chronic and widespread unemployment, should the government provide long-term unemployed adult citizens with the opportunity to do meaningful work at a wage that will keep them out of poverty? Why or why not?

18. Have you used ChatGPT? Where would you draw the line between acceptable and unacceptable uses of generative AI systems like ChatGPT?

19. Some philosophers and computer scientists have argued that because computer programs are not material beings living in the world, they cannot build a model of the world and therefore cannot attain genuine understanding. According to these critics, that is why current AI systems have a problem with truthfulness. What do you think of this argument?

20. Would humans become demoralized by the presence of artificial general intelligence? If so, is it wrong to work on the development of artificial general intelligence?

21. The late theoretical physicist Steven Hawking said the development of a full artificial intelligence could doom the human race. Computer scientist Blaise Agüera y Arcas disagrees, saying that computers are completely dependent on humans for their existence. What do you think?

22. Is it morally acceptable to work on the development of an intelligent machine if it cannot be guaranteed the machine's actions will be benevolent?

23. How will our notions of intellectual property change if computers become capable of creative work?

24. How will our ideas about privacy have to change if legions of superfast computers are analyzing the electronic records of our lives?

25. Kant says that the rationality and autonomy of human beings must always be respected, and that is why people should always be treated as ends in themselves and never merely as the means to an end. Are there any circumstances under which an intelligent computer should be given the same consideration?

26. It is possible to program responses into computers that simulate human emotions. For example, when a computer taking on the role of a nurse hears a parent

say, “My child has diarrhea,” it can respond, “I’m sorry to hear that.” Studies have shown that people can develop an emotional bond with machines that appear to demonstrate human feelings such as empathy. Is it wrong to encourage these attachments by programming computers to mimic human emotions?

27. Would you accept a job that did not have a hybrid work schedule, that is, a job that required you to go into the office every day?

28. *The Grapes of Wrath*, a novel written by John Steinbeck, vividly describes the conditions of migrant workers in California during the Great Depression. In the novel, farmers take advantage of the fact that there is a surplus of labor by lowering wages to the point that families can work all day and still not earn enough money to feed themselves properly. Is the gig economy creating the same kind of “race to the bottom” in terms of worker compensation?

29. A multinational corporation has an office in Palo Alto, California, and an office in Bangalore, India. A 21-year-old American computer science graduate works as a software tester at the Palo Alto office. A 21-year-old Indian computer science graduate has an identical

position at the Bangalore office. The American earns $75,000 per year in salary and benefits; the Indian earns $10,000 per year in salary and benefits. Is this arrangement moral? Should the company give equal pay and benefits for equal work?

30. Do you support the concept of tiered Internet service, providing higher bandwidth to those who pay for premium service?

31. Would the music industry be healthier if winner-take-all effects were reduced? If so, which of the solutions proposed in Section 10.7.2 would make the most sense for the music industry?

32. Should the federal government discourage companies from taking advantage of their salaried employees by requiring firms to pay overtime to any employee who works more than 40 hours in one week?

33. Should all nations sign a treaty banning the development of a new class of weapons—machines exhibiting lethal autonomy—as described in Daniel Suarez's TED Talk?

In-Class Exercises

34. A multinational corporation transfers an employee from India to the United States on an L-1 visa. The employee is a computer programmer, working alongside a US citizen computer programmer doing the same work. Both programmers joined the company five years ago after graduating from college. Their training, skills, and experience are virtually identical.

    Divide the class into groups of four or five students to debate the following proposition: "The salaries and benefits of the two computer programmers should be roughly equivalent."

35. You lead a group of five software engineers involved in the testing of a new product. Your manager tells you that because of a company-wide layoff, you need to give notice to one member of your team. From your interactions with the team members, you can easily identify the two members who are least productive, but you are not sure which of them you should lay off. You know that the company keeps track of all Internet

traffic to each person's computer, although you have never shared this information with your team. You could use this information to determine how much time, if any, these two employees are spending surfing the Web. Is it wrong to access these records?

36. A company runs a large technical support office. At any time, about 50 technical support specialists are on duty, answering phone calls from customers. The company is considering paying the technical support specialists based on two criteria: the average number of phone calls they answer per hour and the results of occasional customer satisfaction surveys. Divide the class into groups of four or five students to debate the pros and cons of the proposed method of determining wages.

37. In this role-playing exercise, students weigh the pros and cons of working for companies with different philosophies about work.

    Company A is a large, established hardware and software company. Employees have a reasonable level of job security, although there have been layoffs in the past few years. Salaries are highly competitive. The company offers stock options, but the stock price is not rising rapidly, and employees know they are not going

to get rich from selling their options. The typical programmer works about 45 hours a week.

Company B is a medium-sized, mature software company that plays a dominant role in a specialized market. The company has never had to lay off employees. Salaries are a little low by industry standards, but programmers get paid overtime when they work more than 40 hours a week. The company discourages managers from resorting to overtime work on projects. Many employees are involved in community activities, such as coaching their kids' sports teams.

Company C is a small start-up company trying to be the first to bring a new kind of shopping experience to the Web. Salaries are not high, but all the employees have a lot of stock options. If the product is successful, everyone expects to become a multimillionaire when the company goes public in a couple of years. In return for the stock options, the founders expect a total commitment from all the employees until the product is released. Every programmer in the company is working 10 hours a day, 7 days a week.

Divide the class into four groups: three groups of recruiters and one group of students about to graduate from college. Each group of recruiters, representing one of the three companies, should make a "pitch" that highlights the reasons why their company represents the best opportunity. The graduates should raise possible negative aspects of working for each company.

38. Divide the class into groups of four or five students to debate the following proposition: "It is immoral for a corporation to pay its chief executive officer (CEO) 670 times as much as a production worker."

References

[1] Vikas Balaj. “A New Capital of Call Centers.” *New York Times*, November 25, 2011.

[2] Don Lee. “The Philippines Has Become the Call-center Capital of the World.” *Los Angeles Times*, February 1, 2015. www.latimes.com/business/la-fi-philippines-economy-20150202-story.html.

[3] Emma Goldberg. “‘Training My Replacement’: Inside a Call Center Worker’s Battle with A.I.” *New York Times*, July 19, 2023. https://www.nytimes.com/2023/07/19/business/call-center-workers-battle-with-ai.html.

[4] “JD. and LL.B Degrees Awarded.” American Bar Association (Web site). Accessed June 11, 2018. https://www.americanbar.org/content/dam/aba/administrative/legal_education_ and_admissions_to_the_bar/statistics/jd_llb_degrees_awarded.authcheckdam.pdf.

[5] “2016 Law Graduate Employment Data.” American Bar Association (Web site). Accessed June 11, 2018. https://www.americanbar.org/content/dam/aba/administrative/

legal_education_and_ admissions_to_the_bar/%20statistics/2016_law_graduate_employment_data.authcheck

[6] Greg Toppo. “Why You Might Want to Think Twice Before Going to Law School.” *USA Today*, June 28, 2017. www.usatoday.com/story/news/2017/06/28/law-schools-hunkering-down-enrollment-slips/430213001/.

[7] “Study Finds ChaptGPT Outperforms Physicians in High-Quality, Empathetic Answers to Patient Questions.” UC San Diego Today, April 28, 2023. https://today.ucsd.edu/story/study-finds-chatgpt-outperforms-physicians- in-high-quality-empathetic-answers-to-patient-questions.

[8] “The 2016 Distressed Communities Index.” Economic Innovation Group. eig.org/wp-content/uploads/2016/02/2016-Distressed-Communities-Index- Report.pdf.

[9] Isaac Asimov. “Runaround.” *Astounding Science Fiction*, 94–103, March 1942.

[10] Kurt Vonnegut Jr. *Player Piano*. Delacorte Press, New York, NY, 1952.

[11] “The Misery of Manufacturing.” *Economist*, 368(8343): 61–62, September 27, 2003.

[12] Todd Lassa. “Toyota, Chrysler Have North America’s Most Efficient Plants.” *Motor Trend* (blog), July 5, 2008. blogs.motortrend.com.

[13] Stanley Aronowitz, Dawn Esposito, William DiFazio, and Margaret Yard. “The Post-Work Manifesto.” In *Post-Work: The Wages of Cybernation*, edited by Stanley Aronowitz and Jonathan Cutler, pp. 31–80. Routledge, New York, NY, 1998.

[14] Michael Gurstein. “Perspectives on Urban and Rural Community Informatics: Theory and Performance, Community Informatics and Strategies for Flexible Networking.” In *Closing the Digital Divide: Transforming Regional Economies and Communities with Information Technology*, edited by Stewart Marshall, Wallace Taylor, and Xinghuo Yu, pp. 1–11. Praeger, Westport, CT, 2003.

[15] Louis Uchitelle and N. R. Kleinfield. “The Price of Jobs Lost.” In *The Downsizing of America*, pp. 3–36. Times Books/Random House, New York, NY, 1996.

[16] Juliet B. Schor. *The Overworked American: The Unexpected Decline of Leisure*. Basic Books, New York, NY, 1991.

[17] Melissa Will. “Hyper Business or Just . . . Hyperbusy.” *Women in Business*, 53(3): 12–15, May/June 2001.

[18] Michael H. Strople. “Bears, Bulls, and Brokers: Employment Trends in the Securities Industry.” *Monthly Labor Review Online*, 128(12): 16–22, December 2005. www.bls.gov.

[19] Martin Carnoy. *Sustaining the New Economy: Work, Family, and the Community in the Information Age*. Russell Sage Foundation/Harvard University Press, New York, NY/Cambridge, MA, 2000.

[20] Steven Rattner. “Full Speed Ahead on A.I. Our Economy Needs It.” *New York Times*, July 10, 2023. https://www.nytimes.com/2023/07/10/opinion/ai-economy-productivity-jobs-workers.html.

[21] The case study is inspired by the following source: Ron Beadle. “Ethics and Employment or the Case of the Cancelled Holiday.” *Second UK Conference on Ethical Issues in Contemporary HRM*, Kingston Business School, January 7, 1998.

[22] Hans Moravec. *Robot: Mere Machine to Transcendent Mind*. Oxford University Press, Oxford, England, 1999.

[23] J. McCarthy, M. L. Minsky, N. Rochester, and C. E. Shannon. “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence.” August 31, 1955. http://jmc.stanford.edu/articles/dartmouth.html.

[24] *Computers and Thought*. Edited by Edward A. Feigenbaum and Julian Feldman. McGraw-Hill, New York, NY, 1963.

[25] “Dendral.” Wikipedia. Accessed July 21, 2023. https://en.wikipedia.org/wiki/Dendral.

[26] William van Melle. “MYCIN: A Knowledge-Based Consultation Program for Infectious Disease Diagnosis.” *International Journal of Man-Machine Studies*, 10(3): 313–332, May 1978.

[27] Peter F. Brown, John Cocke, Stephen A. Della Pietra, Vincent J. Della Pietra, Fredrick Jelinek, John D. Lafferty, Robert L. Mercer, and Paul S. Roossin. “A Statistical Approach to Machine Translation.” *Computational Linguistics*, 16(2), June 1990. https://aclanthology.org/J90-2002.pdf.

[28] “Chinook (Computer Program).” Wikipedia. Accessed July 21, 2023. en.wikipedia.org/wiki/Chinook_(computer_program).

[29] Monty Newborn. *Deep Blue: An Artificial Intelligence Milestone*. Springer, New York, NY, 2002.

[30] "Watson – A System Designed for Answers: The Future of Workload Optimized Systems Design." *IBM Systems and Technology*, February 2011.

[31] Y. LeCun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, and L. D. Jackel. "Backpropagation Applied to Handwritten Zip Code Recognition." *Neural Computation*, 1(4), December 1989.

[32] Paul Mozur. "Google's A.I. Program Rattles Chinese Go Master as It Wins Match." *New York Times*, May 25, 2017. www.nytimes.com/2017/05/25/business/google-alphago-defeats-go-ke-jie-again.html.

[33] "Nearly 1 in 3 College Students Have Used ChatGPT on Written Assignments." Intelligent.com (Web site), January 23, 2023. https://www.intelligent.com/nearly-1-in-3-college-students-have-used- chatgpt-on-written-assignments/.

[34] Stephen Shankland. "AI Gets Smarter, Safer, More Visual with GPT-4 Update, OpenAI Says." *CNET*,

March 15, 2023. https://www.cnet.com/tech/computing/ai-gets-smarter-safer-more-visual-with-gpt-4-update-openai-says/.

[35] Ethan Mollick. “ChatGPT Is a Tipping Point for AI.” *Harvard Business Review*, December 14, 2022. https://hbr.org/2022/12/chatgpt-is-a-tipping-point-for-ai.

[36] Ajay Agrawal, Joshua Gans, and Avi Goldfarb. “ChatGPT and How AI Disrupts Inudstries.” *Harvard Business Review*, December 12, 2022. https://hbr.org/2022/12/chatgpt-and-how-ai-disrupts-industries.

[37] Benjamin Weiser. “Here’s What Happens When Your Lawyer Uses ChatGPT.” *New York Times*, May 27, 2023. https://www.nytimes.com/2023/05/27/nyregion/avianca-airline-lawsuit-chatgpt.html.

[38] Noam Chomsky, Ian Roberts, and Jeffrey Watamull. “Noam Chomsky: The False Promise of ChatGPT.” *New York Times*, March 8, 2023. https://www.nytimes.com/2023/03/08/opinion/noam-chomsky-chatgpt-ai.html.

[39] Tiffany Hsu and Steven Lee Myers. “A.I.’s Use in Elections Sets Off a Scramble for Guardrails.” *New York Times*, June 25, 2023. https://www.nytimes.com/2023/06/25/technology/ai-elections-disinformation-guardrails.html.

[40] Nicholas Nehamas. “DeSantis Campaign Uses Apparently Fake Images to Attack Trump on Twitter.” *New York Times*, June 8, 2023. https://www.nytimes.com/2023/06/08/us/politics/desantis-deepfakes-trump-fauci.html.

[41] Adam Satariano and Paul Mozur. “The People Onscreen Are Fake. The Disinformation Is Real.” *New York Times*, February 7, 2023. https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html.

[42] Joshua L. Kalla and David E. Broockman. “The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments.” *American Political Science Review*, 112: 1, 2018.

[43] Cade Metz. “Internet Companies Prepare to Fight the ‘Deepfake’ Future.” *New York Times*, November 24, 2019. nytimes.com.

[44] Nathan Colaner and Michael J. Quinn. “Deepfakes and the Value-Neutrality Thesis.” Initiative in Ethics and Transformative Technologies, Seattle University, February 10, 2020. https://www.seattleu.edu/ethics-and-technology/viewpoints/deepfakes-and- the-value-neutrality-thesis.html.

[45] “Artificial General Intelligence (AGI).” *Gartner Glossary*. Accessed July 21, 2023. https://www.gartner.com/en/information-technology/glossary/artificial-general-intelligence-agi.

[46] Vernor Vinge. “Technological Singularity.” *Whole Earth Review*, 10, 88–95, Winter 1993.

[47] Cem Dilmegani. “When Will Singularity Happen? 1700 Expert Opinions of AGI [2023].” AIMultiple (Web site), April 28, 2023. research.aimultiple.com.

[48] “Transcript: Ezra Klein Interviews Gary Marcus.” *The Ezra Klein Show*, January 6, 2023. https://www.nytimes.com/2023/01/06/podcasts/transcript-ezra-klein-interviews-gary-marcus.html.

[49] Hubert L. Dreyfus. *What Computers Can’t Do*. Harper & Row, New York, NY, 1979.

[50] Ragnar Fjelland. “Why General Artificial Intelligence Will Not Be Realized.” *Humanities and Social Sciences Communications*, 7(10), 2020. https://doi.org/10.1057/s41599-020-0494-4.

[51] Yoshua Bengio. “One of the ‘Godfathers of AI’ Airs His Concerns.” *Economist*, July 21, 2023. https://www.economist.com/by-invitation/2023/07/21/one-of-the-godfathers-of-ai-airs-his-concerns.

[52] Blaise Agüera y Arcas, Blake Richards, Dhanya Sridhar, and Guillaume Lajoie. “Fears about AI’s Existential Risk Are Overdone, Says a Group of Experts.” *Economist*, July 21, 2023. https://www.economist.com/by-invitation/2023/07/21/fears-about-ais- existential-risk-are-overdone-says-a-group-of-experts.

[53] Anna Jobin, Marcello Ienca, and Effy Vayena. “The Global Landscape of AI Ethics Guidelines.” *Nature Machine Intelligence*, 1: 389–399, 2019. https://doi.org/10.1038/s42256-019-0088-2.

[54] Khari Johnson. “Chatbots Got Big—and Their Ethical Red Flags Got Bigger.” *WIRED*, February 16, 2023.

https://www.wired.com/story/chatbots-got-big-and-their-ethical-red-flags-got-bigger/.

[55] Michael D. Shear. “7 A.I. Companies Agree to Safeguards After Pressure from the White House.” *New York Times*, July 21, 2023. https://www.nytimes.com/2023/07/21/us/politics/ai-regulation-biden.html.

[56] “EU AI Act: First Regulation on Artificial Intelligence.” News release, European Parliament, June 14, 2023. https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial- intelligence.

[57] Sunny Betz. “27 Self-Driving Car Companies You Should Know.” *BuiltIn*, June 29, 2023. https://builtin.com/transportation-tech/self-driving-car-companies.

[58] N. J. Garber and R. Gadiraju. “Factors Affecting Speed Variance and Its Influence on Accidents.” *Transportation Research Record*, 1213, 1989. //onlinepubs.trb.org/Onlinepubs/trr/1989/1213/1213-009.pdf.

[59] Timothy Geary and David Danks. “Balancing the Benefits of Autonomous Vehicles.” In *Proceedings of 2019 AAAI/ACM Conference on AI, Ethics, and Society*, 2019.

[60] Alex London and David Danks. “Regulating Autonomous Vehicles: A Policy Proposal.” In *Proceedings of 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018.

[61] Larry Greenemeier. “Driverless Cars Will Face Moral Dilemmas.” *Scientific American*, June 23, 2016. www.scientificamerican.com/article/driverless-cars-will-face-moral-dilemmas/.

[62] M. Castells. “The Informational Economy and the New International Division of Labor.” In *The New Global Economy in the Information Age: Reflections on Our Changing World*, edited by M. Carnoy, M. Castells, S. S. Cohen, and F. H. Cardoso, pp. 15–43. Pennsylvania State University Press, University Park, PA, 1993.

[63] David Rotman. “How Technology Is Destroying Jobs.” *MIT Technology Review*, 116(4): 27–35, July/August 2013.

[64] Mark Warschauer. *Technology and Social Inclusion: Rethinking the Digital Divide*. MIT Press, Cambridge, MA, 2003.

[65] "Remote Work Frequency Before and After COVID-19 in the United States 2020." *Statista*, July 7, 2023. https://www.statista.com/statistics/1122987/change-in-remote-work-trends-after-covid-in-usa/.

[66] Kim Parker. "About a Third of U.S. Workers Who Can Work from Home Now Do So All the Time." *Pew Research Center*, March 30, 2023. www.pewresearch.org.

[67] "Challenges of Working Remote in 2020." *Statista*, July 7, 2023. https://www.statista.com/statistics/1111401/challenges-of-working-remote-2020/.

[68] Natalia Emanuel, Emma Harrington, and Amanda Pallais. "The Power of Proximity to Coworkers: Training for Tomorrow or Productivity Today?" Working Paper, March 25, 2023. https://scholar.harvard.edu/pallais/publications/power-proximity-office- interactions-affect-online-feedback-and-quits-especially.

[69] David Morel. “Is It the End of Hybrid Working as We Know It?” *Forbes*, June 8, 2023. https://www.forbes.com/sites/davidmorel/2023/06/08/is-it-the-end-of-hybrid-working-as-we-know-it/.

[70] Sarah Kessler. “Getting Rid of Remote Work Will Take More than a Downturn.” *New York Times*, January 7, 2023. https://www.nytimes.com/2023/01/07/business/dealbook/remot work-downturn.html.

[71] Kyle Barr. “Apple Workers Pound the Table for More Work from Home Options.” *Gizmodo*, August 22, 2022. https://gizmodo.com/apple-return-to-office-work-from-home-remote-1849440484.

[72] Mike Rogoway. “Intel Tells Employees It Wants a Better ‘Balance’ on Remote Work.” *OregonLive*, May 10, 2023. https://www.oregonlive.com/silicon-forest/2023/05/intel-tells-employees- it-wants-a-better-balance-on-remote-work.html.

[73] Soumya Karlamangla. “With Commuters Staying Home, Transit Agencies Try to Reinvent Themselves.” *New York Times*, June 19, 2023. https://www.nytimes.com/2023/06/19/us/bart-san-francisco-california.html.

[74] Gerald Friedman. “The Rise of the Gig Economy.” *Dollars&Sense: Real World nomics*, March/April 2014. dollarsandsense.org.

[75] Monica Anderson, Colleen McClain, Michelle Faverio, and Risa Gilles-Watnick. “The State of Gig Work in 2021." *Pew Research Center*, December 8, 2021. www.pewresearch.org/internet/2021/12/08/the-state-of-gig-work-in-2021/.

[76] Natasha Singer. “In the Sharing Economy, Workers Find Both Freedom and Uncertainty.” *New York Times*, August 16, 2014. www.nytimes.com.

[77] Robert Reich. “In Sharing Economy, Workers Get Stuck with the Scraps.” SFGate (Web site), February 7, 2015. www.sfgate.com.

[78] Carolyn Said. “Internal Uber E-mails Reflect Company’s Brash Reputation.” SFGate (Web site), January 30, 2015. www.sfgate.com.

[79] Maya Kosoff. “The California Labor Commission Just Ruled That an Uber Driver Is an Employee—Here’s Why It Could Dramatically Change Uber’s Business Model.” *Business Insider*, June 17, 2015. www.businessinsider.com.

[80] American Management Association. "2007 Electronic Monitoring & Surveillance Survey." February 28, 2008. press.amanet.org.

[81] S. Swanson. "Employers Take a Closer Look." *InformationWeek.com*, 897: 40–41, July 15, 2002.

[82] Rachel Fielding. "Management Week: Web Misuse Rife in UK Firms." VNU NET (Web site), July 15, 2002.

[83] "Stopping Workplace Internet Abuse—First Step Is Identifying Scope of the Problem." *PR Newswire*, October 7, 2002.

[84] Carl Weinschenk. "Prying Eyes." *Information Security*, August 2002.

[85] Melissa Solomon. "Watching Workers: the Dos and Don'ts of Monitoring Employee Productivity." *Computerworld*, July 8, 2002.

[86] Murray Chass. "Umpires Renew Objections to Computer System." *New York Times*, March 4, 2003.

[87] Katie Hafner. "Where the Hall Monitor Is a Webcam." *New York Times*, February 27, 2003.

[88] Sam Dillon. "Classroom Cameras Catch Every Move." *Sunday Oregonian* (Portland, OR), September 28,

2003.

[89] Andrew Urbaczewski and Leonard M. Jessup. "Does Electronic Monitoring of Employee Internet Usage Work?" *Communications of the ACM,* 45(1): 80–83, January 2002.

[90] Robert X. Cringely. "Holy Cow! What Are All These Programmers Doing in India?" *I, Cringely*, PBS, July 10, 1997. www.pbs.org/cringely.

[91] Cindy Easton. "Offshore Software Development: Is It Helping or Hurting Our Economy?" *Cursor* (Software Association of Oregon Newsletter), February 2003.

[92] Patrick Thibodeau. "Survey: One in Four IT Jobs Moving Offshore." *Computerworld*, December 9, 2008. www.computerworld.com.

[93] "One World?" *Economist*, 345(8039): 79–80, October 16, 1997.

[94] Paul Krugman. "Enemies of the WTO; Bogus Arguments Against the World Trade Organization." *Slate*, November 24, 1999. www.slate.msn.com.

[95] Anthony B. Bradley. "Corn Subsidies at Root of US-Mexico Immigration Problems." Acton Institute, February 29, 2012. www.acton.org.

[96] Anthony Perkins. “Investors: Brace Yourselves for the Next Bubble Bath.” *Red Herring*, 21–22, November 13, 2000.

[97] Reuters. “Technology Sector Lost 560,000 Jobs in Two Years.” *NYTimes.com*, March 19, 2003.

[98] Joseph Menn. “Data Reveals Severity of Tech’s Pain.” *Los Angeles Times*, March 7, 2003.

[99] Patrick Thibodeau. “H-1B Visa Count Down, Anger Up.” *Computerworld*, February 3, 2003.

[100] Patrick Thibodeau. “Feds to Research 20,000 H-1B Visas Next Week.” *Computerworld*, May 4, 2005.

[101] Eric Chabrow. “Opposing Views: The Debate over the H-1B Visa Program.” *Information Week*, May 9, 2005.

[102] Department of State. “Nonimmigrant Visas Issued by Classification (Including Border Crossing Cards), Fiscal Years 2012–2016.” travel.state.gov/content/dam/visas/Statistics/AnnualReports/FY2016AnnualReport/FY16AnnualReport-TableXVIB.pdf.

[103] “Chinese Firm Buys IBM PC Business.” *BBC News*, December 8, 2004.

[104] Jeffrey Towson and Jonathan Woetzel. “All You Need to Know About Business in China” (book excerpt), April 2014. www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/all-you-need-to-know-about-business-in-china.

[105] “A Wealth of Choices: From Anywhere on Earth to No Location at All.” ATKearney (Web site), accessed October 29, 2015.

[106] Alban Douillet, Juergen Ributzka, and Suneel Jain. “Open64 Compiler and Tools,” 2015. sourceforge.net/projects/open64/.

[107] Eldon R. Rene, Manivannan Sethurajan, Vinoth Kumar Ponnusamy, Gopalakrishnan Kumar, Thi Ngoc Bao Dung, Kathirvel Brindhadevi, and Arivalagan Pugazhendhi. “Electronic Waste Generation, Recycling and Resource Recovery: Technological Perspectives and Trends.” *Journal of Hazardous Materials*, 416, August 15, 2021. https://www.sciencedirect.com/science/article/abs/pii/S0304389

[108] Tim Johnson. “E-waste Dump of the World.” *Seattle Times*, April 9, 2006. https://web.archive.org/web/20160105213950/http://old.seattle nationworld/2002920133_ewaste09.html.

[109] Jim Puckett, Leslie Byster, Sarah Westervelt, Richard Gutierrez, Sheila Davis, Asma Hussain, and Madhumitta Dutta. "Exporting Harm: The High-Tech Trashing of Asia." *The Basel Action Network (BAN) and Silicon Valley Toxics Coalition (SVTC)*, February 25, 2002. https://noharm-asia.org/sites/default/files/documents-files/84/Exporting_Harm_Trashing_Asia.pdf.

[110] George Monbiot. "From Toxic Waste to Toxic Assets, the Same People Always Get Dumped On." *Guardian*, September 21, 2009. https://www.theguardian.com/commentisfree/cif-green/2009/sep/21/global-fly-tipping-toxic-waste.

[111] L. Guo, W. D. Walls, and X. Zheng. "Waste Import Bans and Environmental Quality: Evidence from China's Electronic Waste Disposal Towns." *Environmental Resource Economics*, 85: 65–108, 2023. https://doi.org/10.1007/s10640-022-00756-0.

[112] Pippa Norris. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge University Press, Cambridge, England, 2001.

[113] Internet World Stats: Usage and Population Statistics. "World Internet Usage and Population Statistics: 2023 Year Estimates" Accessed August 12, 2023. www.internetworldstats.com.

[114] "Countries with Lowest Number of Smartphones per Capital." *WorldAtlas*. Accessed August 12, 2023. www.worldatlas.com.

[115] Elena Murelli. *Breaking the Digital Divide: Implications for Developing Countries*. Edited and with foreword by Rogers W'O Okot-Uma. SFI Publishing, 2002.

[116] Andrew Perrin and Sara Atske. "7% of Americans Don't Use the Internet. Who Are They?" *Pew Research Center*, April 2, 2021. pewresearch.org.

[117] Community College Research Center. "What We Know About Online Course Outcomes." Columbia University, April 2013. ccrc.tc.columbia.edu.

[118] "Broadband Connectivity Competition Policy." Federal Trade Commission, Washington, DC, June 2007.

[119] Jim Louderback. "Winter of My Discontent." *PC Magazine*, April 10, 2007.

[120] S. Derek Turner. “Give Net Neutrality a Chance.” *BusinessWeek Online*, July 12, 2007.

[121] Jeff Sommer. “What the Net Neutrality Rules Say.” *New York Times*, March 12, 2015. www.nytimes.com.

[122] Bill Chappell. “FCC Approves Net Neutrality Rules for ‘Open Internet.’” National Public Radio, February 26, 2015. www.npr.org.

[123] Tom Huddleston, Jr. “Reactions to FCC Net Neutrality Vote: Celebrations, Legal Threats and Morse Code.” *Forbes*, February 26, 2015. fortune.com.

[124] “Broadband for America Statement on FCC Open Internet Order Vote.” February 26, 2015. www.broadbandforamerica.org.

[125] Keith Collins. “Net Neutrality Has Officially Been Repealed. Here’s How That Could Affect You.” *New York Times*, June 11, 2018. www.nytimes.com/2018/06/11/technology/net-neutrality-repeal.html.

[126] Cecelia Kang. “Washington Governor Signs First State Net Neutrality Bill.” *New York Times*, March 5, 2018. https://www.nytimes.com/2018/03/05/business/net-neutrality-washington-state.html.

[127] Rishi Iyengar. “India Now Has the ‘World’s Strongest’ Net Neutrality Rules.” *CNN*, July 12, 2018. https://money.cnn.com/2018/07/12/technology/india-net-neutrality-rules-telecom/index.html.

[128] Alex Hern. “EU Net Neutrality Laws Fatally Undermined by Loopholes, Critics Say.” *Guardian*, October 27, 2015. https://www.theguardian.com/technology/2015/oct/27/eu-net-neutrality- laws-fatally-undermined-by-loopholes-critics-say.

[129] “Net Neutrality by Country.” *Wikipedia*, Accessed July 26, 2023. https://en.wikipedia.org/wiki/Net_neutrality_by_country.

[130] Robert H. Frank and Philip J. Cook. *The Winner-Take-All Society*. Penguin Books, New York, NY, 1995.

[131] “Where’s the Stick?” *Economist*, 13, October 11, 2003.

[132] Sian Boyle. “No More Out of Office? Staff at German Car Giant Daimler to Have Incoming Emails Automatically Deleted During Time Off to Guarantee Peaceful Holidays.” *Daily Mail*, August 14, 2014. www.dailymail.co.uk.

Appendix A

Plagiarism

An ethical analysis of a scenario involving plagiarism appears in Section 2.6.2. This appendix provides a much more

complete picture of what plagiarism is and how to avoid it.

Consequences of Plagiarism

According to the Council of Writing Program Administrators (WPA), "plagiarism occurs when a writer deliberately uses someone else's language, ideas, or other original (not common-knowledge) material without acknowledging its source" [**1**]. The consequences of plagiarism can be severe. Newspaper reporters and college professors have lost their jobs because they plagiarized the work of others [**2**, **3**]. Colleges and universities view plagiarism as a form of cheating. In 2003 at the University of Virginia, 48 students either quit or were expelled for plagiarism [**4**].

The vast amount of information freely available on the Internet, the power of search engines, and the cut-and-paste capability of contemporary computer programs have made it easier than ever to commit plagiarism. Of course, Web search engines can also make it easy for teachers to detect plagiarism [**5**].

Types of Plagiarism

You are plagiarizing if you deliberately do any of the following:

- Copy the words of another without both (1) putting the copied text in quotation marks and (2) citing the source
- Paraphrase the words of another without citing the source
- Incorporate the figures or drawings of another person without crediting the source
- Include facts that are not common knowledge without citing the source
- Use another person's ideas or theories without giving that person credit

Guidelines for Citing Sources

Common knowledge means information that is available in many places and known to a large number of people. For example, it is common knowledge that Delaware was the first

state to ratify the United States Constitution. You do not have to cite a source when presenting common knowledge.

However, you *should* cite a source when you present facts that are not common knowledge. For example, it is not common knowledge that the percentage of college freshmen in the United States interested in majoring in computer science dropped by more than 60 percent between 2000 and 2004 [6].

You must cite a source if you present another person's interpretation of the facts, whether or not you acknowledge the person by name. For example, Cass Sunstein argues that information technology may weaken democracy by allowing people to filter out news that contradicts their view of the world [7]. If you repeat someone else's idea, you must cite where you found it.

How to Avoid Plagiarism

Always put quotation marks around text you have obtained from another source, and write down enough information about the source that you can cite it properly. Do this when you are collecting your notes, so that when you are writing your paper, you will not forget that the words are a direct quotation or whom you are quoting.

When you are paraphrasing the work of another, read over the material, then put it aside before you begin writing. That will help ensure you are using your own words to express the ideas. Check your paraphrase against the source document. Make sure you have not distorted the original meaning. Whenever you have used a phrase from another person's work, you must put the phrase in quotation marks. Always cite the source of the ideas you are paraphrasing, even if there are no direct quotations.

Finally, remember to cite the sources of illustrations and figures that you reproduce.

Misuse of Sources

The WPA definition of plagiarism emphasizes that it is the *deliberate* attempt to conceal the source of the words or ideas. This aligns with our definition of ethics as being focused on the *voluntary* moral choices people make. If a person has no intention of deceiving, but fails to cite sources or use quotation marks correctly, that person's actions constitute **misuse of sources**.

Additional Information

For more information, read “Defining and Avoiding Plagiarism: The WPA Statement on Best Practices,” which is the principal source document for this appendix [**1**].

References

[1] Council of Writing Program Administrators. "Defining and Avoiding Plagiarism: The WPA Statement on Best Practices." January 2003. www.wpacouncil.org.

[2] "Corrections." *New York Times*, May 2, 2003.

[3] Scott Smallwood. "Arts Professor at New School U. Resigns after Admitting Plagiarism." *Chronicle of Higher Education*, September 20, 2004.

[4] Brian Hansen. "Combating Plagiarism: Is the Internet Causing More Students to Copy?" *CQ Researcher* 13(32), 2003.

[5] Katie Hafner. "Lessons in Internet Plagiarism." *New York Times*, June 28, 2001.

[6] Jay Vegso. "Interest in CS as a Major Drops among Incoming Freshmen." *Computing Research News* 17(3), May 2005.

[7] Cass Sunstein. *Republic.com*. Princeton University Press, Princeton, NJ, 2001.

Appendix B

Introduction to Argumentation

B.1 Introduction

The inherent dignity and value of every human being does not mean that everybody's opinions are equally reasonable. Sometimes individuals have viewpoints that are not well thought out, and even when people are being logical, they may not always have a good grasp of the facts. Furthermore, people who want to have their way may express views that they know to be unreasonable.

This appendix is designed to help you make clear and compelling arguments to support your decisions. It will also help you learn how to identify the logical mistakes people can make as they attempt to justify their positions. It illustrates a few of the unfair tactics often employed by debaters trying to undermine the arguments proposed by their adversaries. Finally, it also illustrates how to write persuasive essays based on rigorous arguments.

B.1.1 Arguments and Propositions

We begin by clarifying what we mean by the word "argument." In everyday parlance, "argument" means a heated disagreement. In propositional logic, the word **argument** refers to a set of statements that make and support a claim with respect to a question or issue. We call the meaning of each statement a **proposition**.

A proposition is either true or false; hence statements that express propositions have a truth value. For example, "The Nile River empties into the Mediterranean Sea" expresses a proposition with the truth value of true. The statement, "It has never snowed in Seattle, Washington," expresses a proposition with the truth value of false. "Please take out the garbage" is a command, does not have a truth value, and is not a proposition. For the same reason, the question "How much does that car cost?" does not express a proposition. Statements of opinion, such as "Orange is the best color," are not appropriate for arguments because, while they do express propositions, the truth of the propositions cannot be determined by objective evidence.

Any proposition can be negated, changing its truth value from true to false or from false to true. For example, these statements express the negations of the two propositions appearing in the previous paragraph. "The Nile River does

not empty into the Mediterranean Sea" has the truth value of false. "It has snowed in Seattle, Washington" has the truth value of true.

A **propositional variable** is a symbol representing an arbitrary proposition in an argument. We will use the letters P, Q, and R to represent propositional variables.

The propositions of an argument can be divided into the premises and the conclusion:

- The **conclusion** is the position held by the person making the argument that they hope to persuade others to hold as well. Even though it may appear anywhere in the argument, the conclusion is the end to which the argument is directed.
- The **premises** are the elements from which the conclusion is derived. There are three types of premise:
    - The **grounds** are the facts or pieces of evidence used to support the conclusion. The conclusion of one argument may be incorporated into the grounds of a subsequent argument.
    - The **warrant** is the reason why the truth of the conclusion necessarily follows from the truth of the grounds. In many arguments, the warrant is a

conditional statement of the form "if P, then Q." We call P the **antecedent** and Q the **consequent** of the conditional statement. In some arguments the warrant is implicit and must be deduced from the premises and the conclusion.

- The **backing** provides the justification for the warrant. If the warrant is a conditional statement, the backing explains why the truth of the consequent necessarily follows from the truth of the antecedent.

Here is an example of an argument, with each part of the argument identified:

Angelo posted five photos of his beautiful children on his Facebook page.	*Grounds*
Photos are an example of intellectual property content.	*Grounds*
According to Facebook's "Statement of Rights and Responsibilities,"	*Backing*
if you use Facebook, you grant Facebook a royalty-free license to use	*Warrant*

any intellectual property content you post.

That means Angelo has granted Facebook a royalty-free license to use any of the photos he posted.

Conclusion

B.1.2 Conditional Statements

Under which circumstances is a conditional statement true? Suppose someone tells you, “If you give me $3, I will bring you a cappuccino.” If you give that person $3 and they bring you a cappuccino, then their statement is true. If you give them $3 and they do not bring you a cappuccino, then they were lying, and their conditional statement is false. What if you choose not to give them $3? In that case, you have no right to call them a liar if they don’t bring you a drink, because that action was conditioned on getting $3 from you, and that didn’t happen. To sum up, the only case in which a conditional statement is false is when the antecedent is true and the consequent is false.

More formally, the conditional statement "if P, then Q" (or "P implies Q") is false when P is true and Q is false. The conditional statement is true under any of the other three circumstances, as shown in the following truth table:

P	*Q*	*if P, then Q*
true	true	true
true	false	false
false	true	true
false	false	true

A conditional statement does not have to be expressed exactly in the form "if P, then Q." For example, all three statements below have the same meaning. In the first, the condition is explicit; in the latter two, the condition is implicit:

If x is a bird, then x has wings.

All birds have wings.

Birds have wings.

It's important to remember that the truth of the conditional statement "P implies Q" does not mean that "Q implies P" must also be true. For example, the fact that all birds have

wings does not mean that every winged thing is a bird. (You can probably think of three winged things that are not birds.)

In fact, the conditional statement that *is* logically equivalent to "if P, then Q" is its **contrapositive:** "if not Q, then not P," as demonstrated in the following truth table:

P	*Q*	*if P, then Q*	*not Q*	*not P*	*if not Q, then not P*
true	true	true	false	false	true
true	false	false	true	false	false
false	true	true	false	true	true
false	false	true	true	true	true

See from the table that whenever the conditional statement "if P, then Q" is true, its contrapositive "if not Q, then not P" is true, and vice versa. That means the two conditional statements are logically equivalent.

When we say P is a **sufficient condition** for Q, we mean that the truth of P ensures the truth of Q, as represented by the conditional statement, "If P, then Q."

When we say P is a **necessary condition** for Q, we mean that P must be true in order for Q to be true. In other words, P cannot be false when Q is true; put another way, the truth of Q ensures the truth of P, as represented by the conditional statement, "If Q, then P."

)

B.1.3 Backing

To use a conditional statement effectively as a warrant in an argument, you must be able to justify it to a reasonable yet skeptical audience. It needs backing. The appropriate backing depends upon the type of argument being made, such as a mathematical, scientific, or ethical argument.

Mathematical arguments rely upon mathematical truths to justify warrants expressed as conditional statements. For example, it is a mathematical certainty that for real numbers *a* and *b*, if $a > 0$ and $b < 0$, then the product $ab < 0$.

Warrants in scientific arguments rest upon scientific evidence. For example, we know through repeated experimentation that if you raise the temperature of a pan of water at sea level to 100 degrees Celsius, it will boil.

The warrants in ethical arguments are backed by ethical theories, such as Kantianism, utilitarianism, social contract theory, and virtue ethics. The following warrant, for example, is backed by Kantian ethics: If there is a contradiction between what I wish to do and what I expect

others to do in a similar situation, then what I am considering doing is wrong.

B.2 Valid Arguments

An argument is **valid** if its structure ensures that the truth of the premises makes the truth of the conclusion a logical certainty. Even if an argument is valid, you cannot assume that its conclusion is true; the conclusion is true only if all the argument's premises are true. A valid argument with all its premises true is called a **sound** argument. Four common forms of valid arguments are called affirming the antecedent, denying the consequent, process of elimination, and chain rule.

B.2.1 Affirming the Antecedent (Modus Ponens)

The most direct form of deductive reasoning is called **affirming the antecedent** (or **modus ponens**). It is an argument of the form:

If P, (*warrant*)

then

Q.

P. (*grounds*)

Therefore, (*conclusion*)

Q.

Example 1

By law, if a product does not come with a written warranty, it is still covered by an implied warranty. This thumb drive does not come with a written warranty. Therefore, this thumb drive is still covered by an implied warranty.

Explanation: The first sentence is a conditional statement that serves as the warrant of the argument. The backing for the warrant is the fact that there is a law establishing implied warranties. The second sentence in the argument establishes "this thumb drive" as a product without a written warranty, satisfying the antecedent of the conditional statement. Therefore, the consequent of the conditional statement is

true, as expressed in the argument's third sentence. Note that even if one or both of these premises in this example are not true, affirming the antecedent is a valid argument because its form is correct; namely, if both premises were true, the conclusion would also have to be true.

B.2.2 Denying the Consequent (Modus Tollens)

An indirect form of argument, known as **denying the consequent** (or **modus tollens**), relies upon the contrapositive form of a conditional statement.

An argument based on denying the consequent has this form:

If P, (*warrant*)
then Q.

Not Q. (*grounds*)

Therefore, (*conclusion*)

not P.

Example 2

Responsible personal computer owners keep their computers' security software up-to-date. Sheila has not kept her personal computer's security software up-to-date. Therefore, Sheila is not a responsible personal computer owner.

Explanation: The meaning of the first sentence of the argument is the same as the conditional statement, "If a person is a responsible computer owner, then that person keeps their computer's security software up-to-date." The contrapositive of this statement is, "If a person has not kept their computer's security software up-to-date, they are not a responsible computer owner." The second sentence of the argument establishes Sheila as a person who has not kept her computer's security software up-to-date. Therefore, we know through the contrapositive form of the conditional statement that Sheila is not a responsible computer owner, as stated in the conclusion. Note that in this example the warrant reflects

the opinion of the person making the argument, giving the warrant a weaker justification than if it were based on a mathematical truth or scientific fact.

B.2.3 Process of Elimination

An argument uses the **process of elimination** when it first asserts that at least one of a fixed number of possibilities is true, explains why all but one of the possibilities are false, and concludes that the remaining possibility is true. In the simplest form of this argument, there are only two possibilities, P and Q, and the argument has the form:

P or Q. (*grounds*)

Not P. (*grounds*)

Therefore, Q. (*conclusion*)

Example 3

We have established that the hacker must have been Allen or Barbara. We have also seen incontrovertible evidence demonstrating that Allen was not the hacker. Therefore, the hacker must have been Barbara.

Explanation: The first sentence summarizes an earlier determination that only two people could have been the hacker: Allen or Barbara. The second sentence recalls evidence already presented that eliminates one of the two possibilities—Allen—leaving Barbara as the only remaining possibility. In this argument the warrant is implicit because it is a well-known logical truth: If (P or Q) and (not P) then Q.

B.2.4 Chain Rule

Unlike the arguments already presented, an argument based on the chain rule has two warrants.

Both warrants are conditional statements, and the consequent of the first conditional statement is the antecedent of the second conditional statement. An argument using the chain rule has the form:

If P, (*warrant*)
then
Q.

If Q, (*warrant*)
then
R.

P. (*grounds*)

Therefore, (*conclusion*)
R.

Example 4

If somebody steals something, then that person has broken the social contract. If somebody breaks the social contract,

that person has done wrong. Malik stole a computer. Therefore, what Malik did was wrong.

Explanation: The consequent of the first conditional statement and the antecedent of the second conditional statement match, fulfilling the requirements of the chain rule. The third sentence establishes that Malik stole a computer, satisfying the antecedent of the first conditional statement. Therefore, the consequent of the second conditional statement is true, legitimizing the conclusion stated in the last statement in the argument.

An argument can be expressed in many ways without losing its validity. Here is a rephrasing of the previous example in a more natural style.

Example 5

Stealing is a violation of the social contract, and violating the social contract is wrong. Malik stole a computer. What

Malik did was wrong.

B.3 Unsound Arguments

The conclusion to an argument may be false even if the form of the argument is valid. If all the premises of a valid argument are true, then the argument is sound, but if one of the premises is false, the argument falls apart and is **unsound**.

Example 6

Leroy posted an unflattering photo of Jazmine on his Facebook page. Jazmine did not give Leroy permission to post that photo. It is wrong to post someone's photo on the Web without their permission. Therefore, it was wrong for Leroy to post Jazmine's photo on the Web.

Explanation: The argument is based on affirming the antecedent and is valid. However, if it is not true that Leroy posted Jazmine's photo on his Facebook page, then the argument is unsound. How could that be? Suppose it turns

out that there is no evidence that Leroy posted the photo, other than the observation that Jazmine's photo appeared on Leroy's Facebook page. Perhaps a third party hacked into Leroy's account and posted the photo. If that were the case, the first premise would be false, and the argument would be unsound.

Example 7

A federal court struck down the Federal Communication Commission's net neutrality rules and said the Internet cannot be treated as a Title I service. That means the government can either classify the Internet as a Title II service regulated by the FCC or leave the Internet unregulated. Title II regulations are suitable for radio and television, but not the Internet. Therefore, the government should leave the Internet unregulated.

Explanation: The argument is valid; it is an example of proving something using the process of elimination.

However, the argument is unsound because it contains a false dichotomy: assuming there are only two choices available when there are in fact more. One of the grounds is that the only two options available to the federal government are classifying the Internet as a Title II service or leaving it unregulated. The premise ignores other options available to the federal government: the FCC could appeal the federal court's decision to the US Supreme Court, and Congress could pass a law that the Internet remain a Title I service. The premise is false, and the argument is unsound.

Note that an unsound argument may still have a true conclusion. Consider the following argument.

Example 8

The Internet worm released by Robert Tappan Morris Jr. caused billions of dollars of damage to computer systems with no positive results. Any action that causes billions of dollars of damage to computer systems with no positive

results is wrong. Therefore, Robert Tappan Morris Jr. was wrong to have released the Internet worm.

Explanation: The argument is unsound because it is not true that the Internet worm released by Robert Tappan Morris Jr. caused billions of dollars of damage to computer systems. That does not mean, however, that the conclusion is wrong. Most ethicists would agree that what Morris did was wrong. It simply means that the argument does not prove the conclusion.

B.4 Common Fallacies

In this section, we present several common forms of faulty reasoning, or **fallacies**.

The first two of these fallacies, affirming the consequent and denying the antecedent, are examples of invalid arguments. When an argument is invalid, it is possible that both (a) the premises could be true and (b) the conclusion could be false. To rebut an invalid argument, you do not have to worry about whether the premises are true. Instead, you just name the logical error.

The third fallacy, begging the question, refers to an argument that is (technically) valid and perhaps even sound, but does not perform the function that an argument is supposed to perform: convincing people of something they don't already believe on the basis of things they already do believe. Instead, question beggars present the conclusion as one of the premises, making the argument pointless.

The remainder of the fallacies described in this section are unsound arguments, where at least one of the premises is false.

B.4.1 Affirming the Consequent

Affirming the consequent means assuming that the truth of the consequent of a conditional statement implies the truth of the antecedent; i.e., mistakenly assuming that if P is sufficient for Q (P implies Q) then P is necessary for Q (Q implies P). Affirming the consequent is an invalid argument of the form:

If P, (*warrant*)
then
Q.

Q. (*grounds*)

Therefore, (*conclusion*)
P.

Example 9

People seeking publicity always have Twitter accounts. Joe has a Twitter account. Therefore, Joe must be seeking publicity.

Explanation: The conclusion is not supported by the grounds and the warrant. The warrant states that all people seeking publicity have Twitter accounts. However, even if the warrant were true, that does not imply that all people with Twitter accounts are seeking publicity. There can be other reasons for starting a Twitter account. For example, people interested in getting tweets from public figures also open Twitter accounts. That means having a Twitter account is a necessary, but not a sufficient, condition for demonstrating that a person is seeking publicity. We cannot conclude Joe is seeking publicity simply because he has a Twitter account.

B.4.2 Denying the Antecedent

Another common logical mistake is erroneously assuming that if the antecedent of a conditional statement is false, then the consequent must be false; i.e., assuming that if the antecedent is sufficient for the consequent, then the antecedent must also be necessary for the consequent. The fallacy is called **denying the antecedent**. The argument is of the form:

If A, (*warrant*)
then B.

Not A. (*grounds*)

Therefore, (*conclusion*)
not B.

Example 10

If an employee blows the whistle on corporate wrongdoing, they are shunned by their coworkers. Sadia did not blow the whistle on corporate wrongdoing. Therefore, she is not being shunned by her coworkers.

Explanation: It may be true that whistle-blowers are invariably shunned by coworkers, but people other than whistle-blowers can be shunned. For example, prejudiced people might shun Sadia because she is a devout Muslim. Therefore, the fact that a person is being shunned by coworkers is a necessary but not a sufficient condition to determine that the person is a whistle-blower.

B.4.3 Begging the Question

Begging the question means assuming what you are trying to prove. It is an argument of the form:

P. (*grounds*)

Therefore (*conclusion*)

P.

In other words, the grounds and the conclusion are the same. Begging the question is a logical fallacy because asserting the truth of a claim does not make it true. It is a non-argument dressed up as an argument. Begging the question can be difficult to spot because the same premise is usually expressed in two different ways.

Example 11

Consumers have a right to control who sees their Web browsing data, so Internet Service Providers should have to get permission from consumers before sharing or selling their Web browsing data.

Explanation: Stating that Internet Service Providers should be required to get permission from consumers before sharing or selling their Web browsing data is simply another way of stating that consumers have a right to control who can get access to this information.

B.4.4 Slippery Slope

A **slippery slope** argument claims, without adequate evidence, that a decision with relatively benign consequences will lead to a future event with significant negative consequences.

Example 12

Long asked me if I could help him with a question related to the homework assignment, since it's clear to him I understand the material well. If I help Long, he'll tell the other students in the class, and soon they'll be asking me for help, too. Before you know it, I'll be running study sessions for all the students in all my classes, which will hurt my grades and ruin my chances for getting into graduate school, which would be a disaster. I should avoid doing anything that will keep me from getting into graduate school. Therefore, I shouldn't answer Long's question.

Explanation: The person making the argument claims that a simple act of helpfulness will inevitably lead to the loss of the

opportunity to attend graduate school. The likelihood that helping Long with one question will lead to a cascading series of requests for help as described in the argument is low. Besides, the argument ignores the fact that if requests for help become too burdensome, they can be turned down. To rebut this argument, we demonstrate that one of the conditional statements is false. A good candidate is the implied conditional statement, "If all the students in my class ask for help, I'll end up running study sessions for all of them."

B.4.5 Bandwagon Fallacy

An argument that holds something is true because most people believe it to be true is called the **bandwagon fallacy**. It is a logical fallacy because the truth or falsity of a proposition does not depend upon how many people hold that belief.

Example 13

Senator Smug was the better candidate in the election. He won far more votes than his opponent.

Explanation: The argument contains the implied warrant: "If candidate x receives more votes than candidate y, then candidate x is the better candidate." If by "better" we mean "more highly qualified," then it is not necessarily true that every election is won by the better candidate. Numerous statistical studies have demonstrated that incumbents have a built-in advantage over challengers. In addition, the better candidate is not necessarily the candidate who attracts the most donations and runs the most television advertisements, which have an important influence on election results.

B.4.6 Faulty Generalization (Hasty Generalization)

A **faulty generalization** (or **hasty generalization**) occurs when the person making an argument uses only a few instances of

an event to reach a conclusion about every instance of an event.

Example 14

Our campus bookstore is going to go out of business. I and everyone I know have stopped buying our textbooks at the bookstore and are now buying them online.

Explanation: The grounds—that I and everyone I know are no longer buying textbooks at the bookstore—provide evidence of some loss of bookstore income, but it is far from a conclusive proof. How many other students are doing the same thing? Besides, what percentage of the bookstore's profits come from selling books versus selling apparel and souvenirs?

B.4.7 Division Fallacy

Concluding that every member of a group has a property because the property is possessed by the group collectively is called the division fallacy.

Example 15

Global shipments of personal computers declined between the third and fourth quarters of 2016. Therefore, Lenovo's shipments of personal computers declined between the third and fourth quarters of 2016.

Explanation: The conclusion does not necessarily follow from the premise. It is possible for one company to grow its market share and ship more units even when the total number of shipments for all companies is shrinking.

B.4.8 The Fallacy of Equivocation

The **fallacy of equivocation** is when the soundness of an argument relies upon a word or phrase being ambiguous or having multiple meanings.

Example 16

The PC industry is suffering from a lack of innovation. Lenovo is the leader of the PC industry. Leaders are responsible for the performance of their groups. Therefore, Lenovo is responsible for the lack of innovation in the PC industry.

Explanation: In the second sentence the word “leader” refers to Lenovo’s position as #1 in the world with respect to PC sales. In the third sentence the word “leader” refers to a person overseeing the work of a group of people. Because the meaning of the word “leader” in the warrant (the third sentence) is different from the meaning of the word “leader”

in the second premise, the conclusion does not logically follow from the premises and the warrant.

B.5 Unfair Debating Gambits

In a fair debate between two people A and B, person B should be addressing the argument advanced by person A, and vice versa. If one person proposes an invalid argument, the other person should point that out. If both arguments are logically valid, then each person should attempt to demonstrate that the other's argument is unsound by pointing out which premise or premises are false.

Too often, however, debaters do not focus on the actual arguments presented by their adversaries. Instead, they take the easy way out and attempt to influence the audience by introducing irrelevant topics, concocting a distorted version of their opponents' arguments, or attacking their opponents' credibility. In this section, we consider these three unfair debating gambits.

B.5.1 Red Herring

A **red herring** is an irrelevant topic introduced into a debate with the purpose of distracting attention from the original argument.

Example 17

> Aanya: It was morally wrong for you to copy answers from someone else's exam.
>
> Benjamin: What makes something morally wrong?
>
> Aanya: Something is wrong if it goes against a moral code.
>
> Benjamin: Who creates the moral code?

Explanation: In this debate Benjamin has introduced a red herring—the origins of moral codes—to divert the argument from its original focus: the morality of copying exam answers.

B.5.2 Ad Hominem Argument

"Ad hominem" is Latin for "to the person," and it refers to a response that praises or attacks the person making an argument rather than focusing on the premises or the warrants supporting a conclusion. An **ad hominem** argument is a variant of a redherring argument because it changes the focus of the debate: in this case, to the person delivering the message rather than the message itself. The correctness of an argument has nothing to do with the identity of the person communicating it. An evil or ignorant person can make a sound argument, and a good or educated person can make an unsound argument.

Example 18

Anthony (to the audience): Tesla Motors should not have allowed its cars to travel over the speed limit when under the control of Autopilot. For this reason alone, Tesla Motors

bears some moral responsibility for the death of Joshua Brown.

Bernadette (to the audience): What does Anthony know about moral responsibility? He never even took an ethics class!

Explanation: Instead of addressing the issue of whether Tesla should have allowed its cars to travel over the speed limit under the control of Autopilot, Bernadette has shifted the focus to Anthony's credentials for making ethical arguments. The soundness of Anthony's argument does not depend upon Anthony's educational credentials.

B.5.3 Attacking a Straw Man

Another common unfair debating tactic is to mischaracterize the opponent's position to attack it more easily. **Attacking a straw man** means making an argument that refutes an

extreme version of an opponent's position rather than the opponent's actual position.

Example 19

Margarita (to the team): We need to make our computer network more secure by investing in a firewall that will limit access to sites outside our company.

Kim (to the team): The only way to make a local area network totally secure is to disconnect it from the Internet. But then our computers will no longer be useful to us in our work. If we take Margarita's suggestion, we won't be able to get any work done.

Explanation: Kim is attacking a straw man because Margarita was not proposing the drastic action of disconnecting the local area network from the Internet.

)

B.6 Writing Persuasive Essays

An essay is a short piece of writing designed to persuade the reader to agree with a position held by the author. A good persuasive essay contains a sound argument, but also explains why opposing arguments are unsound. Here is one way to structure a persuasive essay, based on the model of argumentation developed by British philosopher Stephen Toulmin [1]:

- Begin with an introduction that presents the topic, explains its relevance, and states the conclusion.
- Present the grounds, the facts upon which the conclusion rests.
- State the warrant or warrants that connect the grounds to the conclusion. Justify each warrant by stating its backing.
- Introduce qualifiers that limit the scope of the conclusion, since most conclusions are not true in all circumstances.

- Present arguments that disagree with the conclusion of the essay and provide evidence to rebut each of them.
- Repeat the conclusion.

What follows is a short persuasive essay based on the Toulmin method. The essay is in the left column, while the right column explains the parts of the essay.

The Government Should Ban Self-Driving Cars

Over the past several decades, advances in hardware and software have enabled automakers to introduce a variety of safety devices into their products. An early example is anti-lock braking systems, designed to prevent skidding on slippery roads by preventing the wheels from locking up when the driver applies the brakes. Anti-lock brakes are now an accepted safety feature of modern automobiles. In the past few years,

The first paragraph introduces the general topic area: the introduction of hardware and software systems into automobiles to improve their safety.

car manufacturers have begun introducing far more sophisticated safety systems. Toyota's Safety Sense, for example, has dynamic radar cruise control to maintain a safe distance with the preceding car, a pre-collision system that can apply the brakes if it detects a potential frontal collision, and a lane-departure alert system.

In 2015 Tesla Motors announced Tesla Version 7.0, a system allowing the Model S sedan to control its speed and steer [**2**]. With Autopilot, the Tesla S became a self-driving vehicle: a vehicle capable of driving itself for extended periods of time in ordinary circumstances, but relying upon a human driver to resume control when necessary. Tesla Motors touted the introduction of Autopilot as a big step forward in automobile safety [**2**].

The second paragraph focuses on the specific topic of the essay: the safety of self-driving automobiles.

Tesla's claims were premature. I argue self-driving cars are inherently unsafe and should be banned by the government.

Conclusion

On May 7, 2016, Joshua Brown was killed when the Tesla he was driving crashed into a semitrailer truck. The accident occurred on a divided highway with the two vehicles traveling in opposite directions. The truck made a left-hand turn in front of Brown's car, and Brown's car drove under the semitrailer portion of the truck, shearing off the roof of the car and killing him. An investigation by the National Traffic Safety Board revealed that Autopilot had been engaged for 37 minutes before the collision, and during this time Brown had had his hands on the steering wheel for only 25 seconds. Neither Brown nor Autopilot

Grounds

applied the brakes before the vehicles collided [3].

Data used to establish truth of the grounds in the next paragraph

Several months before the accident that killed Joshua Brown, Ford Motor Company announced the results of a test determining how long it takes a driver to regain attention and resume control of a self-driving vehicle. The test revealed that it takes anywhere from 3 to 10 seconds for a driver to be ready to take back control. This is called "the hand-off problem" [4].

Denying the consequent

In some emergency situations, to avoid a life-threatening injury, the driver has only a second or two to take corrective action. If the driver cannot take corrective action in two seconds or less, the driver cannot avoid a life-threatening injury. Ford's experiments on the handoff problem demonstrate that drivers of

self-driving cars under computer control do not typically retake control in less than three seconds. What this means is that in some emergency situations, the drivers of self-driving cars will not be able to avoid a life-threatening injury.

Any product that can cause a life-threatening injury when used as designed is a dangerous product. We have established that self-driving cars, when used as designed, can cause a life-threatening injury. Therefore, self-driving cars are dangerous.

Affirming the antecedent

Governments should ban products that are dangerous even when used as designed. Self-driving vehicles are dangerous even when used as designed. Therefore, governments should ban self-driving vehicles.

Affirming the antecedent

Some might argue that governments do not ban cigarettes, even though

Counterclaim

they have been shown to cause harm to the people who smoke them, so why should governments ban self-driving vehicles?

However, second-hand smoke can harm nonsmokers, and for that reason governments do place restrictions on where people can smoke in public. Cars travel on public roads, and an accident with a self-driving car can injure other drivers or pedestrians in addition to the driver of the car. Banning self-driving cars would be consistent with governments banning cigarette smoking in restaurants and classrooms.

Rebuttal

It is worth noting that the hand-off problem is not an issue for fully autonomous vehicles that do not rely upon a human driver to take over when necessary.

Qualifier

However, to promote public safety, governments should ban manufacturers from selling automobiles with self-driving capabilities, unless they are fully autonomous.	*Final claim with qualification*

Quiz

For each of the following arguments, determine whether it is valid. If the argument is valid, identify the argument as valid and name the form of the argument (affirming the antecedent, denying the consequent, process of elimination, or chain rule). If the argument is fallacious, identify the argument as fallacious and name the fallacy (affirming the consequent, denying the antecedent, begging the question, slippery slope, bandwagon, faulty generalization, division, equivocation).

1. When a company adds more automation to one of its factories, it lays off workers. Magma Motors just laid off workers, so it must have added some more automation to one of its factories.

2. John met Mark and pretended to be his friend because he knew Mark could get him a job at Mark's company. According to the Categorical Imperative, it is wrong for one person to treat another person only as a means to an end. Therefore, according to the Categorical Imperative, what John did was wrong.

3. A software engineer at Google wrote a memo arguing that differences of preferences between men and women may explain why women aren't equally represented in the tech industry [5]. Every major news organization wrote an editorial stating that the memo perpetuated gender stereotypes. Thus, it is clear the software engineer's memo perpetuated gender stereotypes.

4. All Alacrity CPUs are designed either to optimize performance or to optimize power consumption. Alacrity's Alpha processor is not designed to optimize performance. Therefore, the Alpha processor is designed to optimize power consumption.

5. Brandon just graduated from East Dakota State University with a B.S. in computer science. Every person graduating from East Dakota State University this year with a B.S. in computer science has received at

least one job offer. Therefore, Brandon has received at least one job offer.

6. Salaries in the computer industry have been rising steadily over the past two years. Ram has been a software engineer at the same company for the past two years. Therefore, Ram is earning more now than he did two years ago.

7. Women are underrepresented in positions of leadership in the tech industry because men hold most of the leadership positions, and when there is an open leadership position, they are more likely to hire a man than a woman.

8. Misaki saved $20 by copying a DVD from a friend. Copying a DVD is a violation of copyright law. Under social contract theory, it is wrong to break the law unless there is an overriding moral reason. Therefore, under social contract theory, Misaki did something wrong.

9. Nobody reads a program's terms and conditions from beginning to end before agreeing to them. I have never met anyone who has read a program's terms and conditions in their entirety.

10. According to John Rawls, in order to be just, any social and economic inequalities must be "to the greatest benefit of the least-advantaged members of society" [6]. Poor people pay a higher percentage of their income in sales taxes than rich people. The inequality caused by sales taxes is not to the greatest benefit of the least-advantaged members of society. Therefore, according to John Rawls, sales taxes are unjust.

11. The scores the students got on the latest homework assignment were much lower than average, but if I let them do the assignment again, they will want to be able to redo every assignment until the end of the semester. They will not take their homework seriously the first time they turn it in, and I will end up grading every assignment twice. For these reasons, it would be wrong for me to let the students do the latest homework assignment again.

12. If you consistently tell the truth for an extended period of time, you will acquire the character trait of honesty. Honesty is not one of Diego's character traits. That means he has not consistently told the truth for an extended period of time.

Answers to the Quiz Questions

1. Fallacious: affirming the consequent. Adding automation results in laid-off workers, but workers can be laid off for other reasons, too. For example, Magma Motors may have laid off workers because sales are down.

2. Valid: affirming the antecedent. The second sentence, the warrant and backing of the argument, contained an implied conditional statement: If person A treats person B only as the means to an end, then person A has done wrong.

3. Fallacious: bandwagon. The fact that many editorialists believe what the software engineer did was wrong does not prove that he did anything wrong.

4. Valid: process of elimination.

5. Valid: affirming the antecedent.

6. Fallacious: division fallacy. The fact that average salaries have risen over the past two years does not mean that Ram's salary has gone up.

7. Fallacious: begging the question. Stating that men hold most leadership positions and usually fill open positions with men is simply another way of saying that women are underrepresented.

8. Valid: chain rule. The argument contains two implied conditional statements. The second sentence of the argument could be phrased, “If you copy a DVD, then you have violated copyright law.” The third sentence contains a backing and a warrant. The warrant can be expressed as a conditional statement: “If you break the law without an overriding moral concern, then you have done something wrong.”

9. Fallacious: faulty generalization. The fact that some people have not read the terms and conditions in their entirety does not prove that everyone has acted the same way.

10. Valid: denying the consequent.

11. Fallacious: slippery slope. The argument claims without proof that the chain of negative consequences is inevitable.

12. Valid: denying the consequent.

Answers to the Quiz Questions

1. Fallacious: affirming the consequent. Adding automation results in laid-off workers, but workers can be laid off for other reasons, too. For example, Magma Motors may have laid off workers because sales are down.

2. Valid: affirming the antecedent. The second sentence, the warrant and backing of the argument, contained an implied conditional statement: If person A treats person B only as the means to an end, then person A has done wrong.

3. Fallacious: bandwagon. The fact that many editorialists believe what the software engineer did was wrong does not prove that he did anything wrong.

4. Valid: process of elimination.

5. Valid: affirming the antecedent.

6. Fallacious: division fallacy. The fact that average salaries have risen over the past two years does not mean that Ram's salary has gone up.

7. Fallacious: begging the question. Stating that men hold most leadership positions and usually fill open positions with men is simply another way of saying that women are underrepresented.

8. Valid: chain rule. The argument contains two implied conditional statements. The second sentence of the argument could be phrased, “If you copy a DVD, then you have violated copyright law.” The third sentence contains a backing and a warrant. The warrant can be expressed as a conditional statement: “If you break the law without an overriding moral concern, then you have done something wrong.”

9. Fallacious: faulty generalization. The fact that some people have not read the terms and conditions in their entirety does not prove that everyone has acted the same way.

10. Valid: denying the consequent.

11. Fallacious: slippery slope. The argument claims without proof that the chain of negative consequences is inevitable.

12. Valid: denying the consequent.

References

[1] Stephen Toulmin. *The Uses of Argument*. Cambridge University Press, USA, 1958.

[2] The Tesla Team. "Your Autopilot Has Arrived." Tesla Motors (blog), October 14, 2015. http://www.tesla.com/blog/your-autopilot-has-arrived.

[3] Joseph A. Gregor. "Driver Assistance System: Specialist's Factual Report." National Transportation Safety Board, March 7, 2017.

[4] Alex Davies. "Ford's Skipping the Trickiest Thing about Self-Driving Cars." *Wired*, November 10, 2015.

[5] Anonymous. "Google's Ideological Echo Chamber." *WorldNetDaily.com*, August 5, 2017. http://www.wnd.com/2017/08/googles-ideological-echo-chamber/.

[6] John Rawls. *Justice as Fairness: A Restatement*, pp. 42–43. Belknap Press of Harvard University Press, Cambridge, MA, 2001.

Index

Numbers

51% attack, 117

60 Minutes, 140

911 services, 239

A

A-0 system, 12

Ababa, Addis, 386

Abacuses, 5

Abel, 62

Abelson, Hal, 211

Abelson, Harold, 259

Abernathy, Ralph, 281

Abraham, 62

Absolute rights, 81

Accolade company, 198

Accreditation, 415–416

ACLU (American Civil Liberties Union)

AIT scanners, 303–304

CIPA, 133

license plate scanners, 276

medical records, 243

National Security Letters challenge, 286–287

Patriot Act, 286–287

Real ID Act, 297–298

surveillance cameras, 275

TALON database, 282

ACM (Association for Computing Machinery) Collegiate Programming Contest, 486

Act utilitarianism, 70

case against, 74–75

case for, 73

ethical evaluations canceled vacation, 463–464

CIPA, 133–134
Firesheep case, 320–321
freedom of expression, 130–131
law breaking, 95–96
spam, 110
Principle of Utility, 70–71
scenario evaluation, 72–73
Acxiom data broker, 249, 253
Ad-blocking software, 152
Ad Hominem argument, 529
Addiction
Internet contributing factors, 145
ethical evaluation, 145
reality of, 144, 145
online games, 114
Adding machines, 7
Address book iPhone uploads, 254–255
Addresses

email, 107

URLs, 112

Adobe, 171

Advanced imaging technology (AIT) scanners, 303–304

Advanced Research Projects Agency (ARPA), 25

Advertising restrictions, 128

Adware, 330

AECL (Atomic Energy of Canada Limited), 368–374

Agents in virtue ethics, 91–92

Agfa Monotype Corporation, 173

Agricultural Commodities Exchange, 117

Aguilera, Christina, 187

AI (artificial intelligence), 465

Air traffic control system failure, 357

Airbnb company, 479

AIT (advanced imaging technology) scanners, 303–304

Al Jazeera, 118

Albrecht, Bob, 16

Aldred, Ruth, 443, 444

Alfred P. Murrah Federal Building bombing, 273

Algorithmic bias, 389

computer systems bias, 389–390

predictive policing, 392–394

Alice Corporation v. CLS Bank, 202–203

Allen, Paul, 16

Alpert, Phillip, 135

Alphabet, Greek, 4, 28

Altair 8800 computer, 16

Alto computer, 31

Amazon.com

customer profiles, 237

information storage by, 284

music sales, 188, 197

video service, 197

wrong prices on, 358

Amber, 18

America Online (AOL)
search dataset, 252
American Civil Liberties Union (ACLU)
AIT scanners, 303–304
CIPA, 133
license plate scanners, 276
medical records, 243
National Security Letters challenge, 286–287
Patriot Act, 286–287
Real ID Act, 297–298
surveillance cameras, 275
TALON database, 282
American Library Association CIPA, 133
Patriot Act resolution, 288
tiered services opposition, 492
American Management Association survey, 481
American Psychiatric Association, 144

American Society of Composers, Authors, and Publishers (ASCAP), 174

Ames Laboratory, 31

Amish, 2

Analog Devices company, 482

Ancheta, Jeanson James, 335

Anderson show, 142

Android operating *system*, 199

Android smartphones, 202

AnnualCreditReport.com site, 293

Anons, 340–341

Anonymized datasets, 251–252

Anonymous group, 340–341

Anti-Phishing Working Group (APWG), 336

Antimalware tools, 332

Antivirus software, 324–325

Antiwar activities, 15

Antiworm scenario, 431–433

AOL (America Online)
search dataset, 252
Apache web server, 209
Apollo player piano, 175
Appalachian Spring, 210
Apple Computer, Inc. v. Franklin Computer Corp., 198
Apple computers development of, 17–18
EMI agreement, 190
FairPlay system, 197
Franklin Computer lawsuit, 198
hypertext *systems*, 32
Macintosh, 32
music service, 197
smartphone patents, 202
Apple iPhone, 202
ApplyYourself software, 318
Apps, 112

APT1 (advanced persistent threat 1) group, 340

APWG (Anti-Phishing Working Group), 336

Arab Spring uprisings, 118, 341

Arete, 86

Argumentation

    backing, 520

    conditional statements, 518–519

    ethical theories, 520

    fallacies, 524–528

    and propositions, 517–518

    unfair debating gambits, 528–529

    unsound, 523–524

    valid, 520–522

    writing persuasive essays, 530

Ariane satellite launch device, 360

Aristotle, 86–88

Arithmometers, 6

Armstrong, Neil, 23

Arnold, Thelma, 252

Aronowitz, Stanley, 460

ARPA (Advanced Research Projects Agency), 25

ARPANET, 25

Arrests, false, 354

Arriba Soft Corporation, 185–186

Ars Technica, 316–318

Articles of Confederation, 127

Artificial general intelligence (AGI), 472–473

Artificial intelligence (AI) systems, 465

    bias in training data sets, 390

    ethics of, 473–475

ASCAP (American Society of Composers, Authors, and Publishers), 174

Asimov, Isaac, 458

Assange, Julian, 341

Assembly language, 12–13

Association for Computing Machinery (ACM) Collegiate Programming Contest, 486

"As We May Think" (Bush), 30–31

Atanasoff, John, 9

Atanasoff-Berry Computer, 9

Atlas Shrugged, 62

Atomic Energy of Canada Limited (AECL), 368–374

AT&T long distance network collapse, 361

    semiconductor development, 13

Attachments, viruses in, 338

Attacking a straw man, 529

Audio collages, 187

Audio Home Recording Act, 184

Audits, IRS, 293

Augmentation Research Center, 31

Authors Guild v. Google, 186–187

Automation

    jobs gained from, 461–462

jobs lost from, 459–460
productivity changes from, 462–463
supply-chain, 477
Automobiles, 3
black boxes, 243
OnStar *system*, 242–243
thefts, 355
Autopilot hand-off problem, 376
May 2016 Fatal Accident, 375–376
moral responsibility, 377–378
SAE Level, 374–375
Avalanche Gang, 336
AVS WinVote DRE system, 366
Aziz, Joseph, 149

B

Babbage, Charles, 6
Backdoor Trojans, 329

Background checks, 238, 250

Backus, John, 12

Bad patents, 201

BAE Automated Systems, 363, 364

Baez, Joan, 281

Baggage handling systems, 363

Ballistic missiles, 14

Band-Aid brand, 171

Bandwagon fallacy, 526–527

Bangalore, 482

Banks, social network data collection by, 57

Baran, Paul, 25

Basic input/output system (BIOS), 199

BASIC interpreter, 16

BASIC programming language, 13

Batteries, invention of, 18

Bay Area Rapid Transit (BART), 151

BBC News, 125

BBN, 25

Beacon *ad system*, 253–254

Beatles, 187

Beijing, 125

Beings in act utilitarianism, 71

Bell, Alexander Graham, 20–22, 172

Bell, Carlos G., Jr., 447

Bell Labs, 13

Bell Telephone Company, 172–173

Bellair, Robert, 306

Bentham, Jeremy, 70, 133

Berners-Lee, Tim, 33, 111

Berry, Clifford, 9

Bharti Airtel, 250

Bias, algorithmic, 389–397

Bible

    in divine command theory, 59–62

    Gutenberg, 29

Biden, Joe, 119

Biggar, Sharon, 254

Bill of Rights

First Amendment, history of, 128

Third Amendment, 231

Fourth Amendment electronic surveillance, 278–282

Patriot Act, 287

Billing errors, 356–358

Biloxi school district, 481

BIND program, 209

BIOS (Basic input/output system), 199

Bitcoin, 115

BitTorrent networks, 194–195

Black Album, The, 187

Black boxes, automobile, 243

Blacklists for Web filters, 132

Blaster worm, 76

Block, Jerald, 143

Block miners, 116

Blogs, 113

Blue Chip Marketing Worldwide, 249

Blue Frog bot, 335

Blue laws, 496

Blue Security, 335–336

BMI, 174

Body scanners, 240–241

Boeing 737 MAX, 381

    background of, 381–382

    consequences of Lion Air and Ethiopian Airlines, 385–387

    Ethiopian Airlines Flight 302, 386

    financial impact of crashes, 388

    lack of full disclosure, 383–384

    Lion Air Flight 610, 384

Boisjoly, Roger, 441, 442

Bookkeepers, 6, 7

Books, fair use, 186–187

Boone County voting machine errors, 366

Booz Allen Hamilton, 283

Bork, Robert, 300

Boston Tea Party, 231

Bot herders, 108, 330, 334

Bots and botnets, 330–331

Boyle, James, 211

Brand, Stewart, 15

Brand names, 171

Brandeis, Louis, 231–232, 279

Brauneis, Robert, 169

Brazil, direct recording voting machines in, 365

Breaking laws, 93–96

in act utilitarianism, 95–96

in Kantianism, 94–95

in rule utilitarianism, 96

in social contract theory, 94

Breyer, Stephen, 169

Bricklin, Dan, 17

BrightLocal survey, 137

Bring your own device (BYOD) movement, 332

Broadband connections, 27

Broadband for America, 492

Brooklyn Bridge, 282

Brooks, Linda, 356

Brooks Brothers, 241

Brown, Laura Clark, 262

Brown, Peter, 32

Browsers

Firesheep, 320–322

first, 33

Brunner, John, 325

Brute-force password attacks, 316

Bryan, William Jennings, 22

Buchanan, Vern, 366

Buchwald, Art, 170

Bugs, 278

Bullying, cyberbullying, 141–142

Burroughs Adding Machine Company, 7

Burroughs, William, 7

Bush, George W., 307

    Florida vote count, 23

    NSA wiretapping, 281

    Real ID Act, 297

Bush, Vannevar, 30–31

Busicom company, 14

Business promotion, Twitter for, 118

Business Week, 318

Butler, Alan, 269

Butler, Eric, 320

C

Cadence Design Systems, 482

Cain, 62

Cairo protests, 118

Calculators, mechanical, 4–6

CALEA (Communications Assistance for Law Enforcement Act), 284–285

CALM Act (Commercial Advertisement Loudness Mitigation Act), 302

Cambridge Analytica, 255–257

Cambridge University, 10

Cameras, closed-circuit, 275–276

CAMI (Columbia Artists Management, Inc.), 174

Campaign finance reform, 496

Campana, Thomas, 201

Canadian parliament, 465

Canter, Laurence, 107

Carlin, George, 129

Carnegie Mellon University, hacked systems at, 319

Carnivore system, 281

Carnoy, Martin, 42, 41

Carpenter v. United States, 301–302

Cash registers, 7, 8

Categorical Imperative, 65–67

Causal condition for moral responsibility, 374

Causal responsibility, 447

CBS election predictions, 11

CDA (Communications Decency Act), 125

CDT (Center for Democracy and Technology), 284

Cell phones dependence on, 2–3

    enhanced 911 services, 239

    subscribers, 250

    tracking, 254

    wireless networks, 27

Censorship, 122

China, 125

direct, 123

ethical perspectives on, 125–127

on Internet, 124

self-censorship, 123–124

Census Bureau, U.S. early computer use, 8, 10–11

records kept, 271–272

Center for Democracy and Technology (CDT), 284

Central Intelligence Agency, 281

CEO pay compared to production workers, 494

Cerf, Vinton, 25

CERN, 33, 111

Certification, 415, 416–417

Certified Public Accountants (CPAs), 416

CETUS (Consortium for Educational Technology in University Systems), 182

CGR corporation, 368

Chain rule, 522

Challenger disaster, 441–442

Chancellor, Joseph, 256, 257

Charles Katz v. United States, 280

Charlie Hebdo, 341

ChatGPT, 467–471

Chess program, 465

Child Internet Protection Act (CIPA)

    ethical evaluation of, 133–134

    passed, 125

Child Online Protection Act, 125

Children, 132

    and online predators, 137–138

    and pornography, 125, 430–431

    Web filters for, 135

Children's Online Privacy Protection Act (COPPA), 271

Chin, Denny, 187

China

    dictatorships, 484

gaming, 147

IBM assets acquired by, 486

Internet access, 124

Internet addiction, 143

unlicensed software, 35

Chinook checkers-playing program, 465

Chips

hybrid, 442–443

implanted, 242

Chowdhury, Abdur, 252

Christianity, 59

Chrome browser, 33

Church, Christian and divine command theory, 59

Church of Scientology, 340

CIA, 281

Cigarette advertising, 128

CIPA (Child Internet Protection Act)

ethical evaluation of, 133–134

passed, 125

Circuit-switched networking, 25

Cisco Systems

India offices, 482

stock prices, 484

Citibank, India offices, 482

Citing sources, 514

Civil Rights Act, 437

Civil War, 272, 444

Clark, Melville, 175

Clay, Henry, 20

Clean room software development, 199

ClearType technology, 173

Cleaver, Eldrige, 281

Cleveland web site, 341

Client principles in Software Engineering Code of Ethics, 420–421

Clinton, Hillary, 120, 151

Closed platform, 207

Closed-circuit television cameras, 275–276

Cloud storage services, 191

CLS Bank, 202

CNN, self-censorship by, 123

COBOL programming language, 13

Coca-Cola, 170–171

Code of Fair Information Practices, 290–291

Code reuse dangers, 373

Codes of ethics. *See* Software Engineering Code of Ethics and Professional Practice

Codices, 29

Coercive Acts, 231

Cohen, Bram, 194

Collaborative filtering, 246

Collage, audio, 187

Colleague principles in Software Engineering Code of Ethics, 424–425

Colleges, contingent faculty members in, 479

Collegiate Programming Contest, 486

Collingwood, Charles, 11

Colonial pipeline, 336–337

Coloniality, 37

Columbia Artists Management, Inc. (CAMI), 174

Com Score survey, 192

Combat Methamphetamine Epidemic Act, 303

Coming to America, 170

Commercial Advertisement Loudness Mitigation Act (CALM Act), 302

Commercial computers

    first, 10–12

    precursors, 9–10

Commercials, loud, 302

Committee on Privacy, 291

Common knowledge, 514

Common Law courts, 127

Commons, 211–213

Communications Assistance for Law Enforcement Act (CALEA), 284–285

Communications Decency Act (CDA), 125

Communities

costs and benefits of, 47

online, 22

Community College Research Center, 491

Comparative advantage, 483

COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), 394-395

Compilers

developed in China, 486

GNU, 209

Complex Number Calculator, 24

Compression algorithms, 184

Computer crime

hackers. *See* Hacking

identity theft. *See* Identity theft

online predators, 137–138

Computer Fraud and Abuse Act, 142, 317, 327

Computing milestones

calculation aids, 4–5

cash registers, 7–8

commercial computer precursors, 9–10

commercial computers, 10–12

IBM System/360 computers, 14

mechanical calculators, 6–7

microprocessors, 14–15

personal computers, 15–18

programming languages and time-sharing, 12–13

punched card tabulation, 8–9

transistors and integrated circuits, 13–14

Concentration camps, 413

Conditional statements, 518–520

Conditions for moral responsibility, 373–374

Confidentiality, 167, 170–171

Conflict of interest scenario, 429–430

Consequentialist theories, 71

Conspiracy Theory, 140

Constitution of the United States

- First Amendment
  - history of, 127–128
  - limitations, 128
- Third Amendment, 231
- Fourth Amendment
  - AIT scanners, 303–304
  - electronic surveillance, 278–282
  - Patriot Act, 287
- Fourteenth Amendment, 447

Consulting opportunity case study, 433–435

Consumption taxes, 496

Contexts in cultural relativism, 56–59

Contingent faculty members, 479

Control systems, 339

Cook, Philip, 493–496, 498

Cookies, 244

Cooper, Anderson, 142

Cooperative agreements for winner-take-all effects, 496

Copland, Aaron, 210

COPPA (Children's Online Privacy Protection Act), 271

Copyright Act of 1909, 176

Copyright Act of 1976, 197–198

Copyright creep, 175–176

Copyright Office, 197–198

Copyright Term Extension Act, 175–176

Copyrights

    extensions, 175–176

    litigation, 173–176

    principle rights, 173–174

    software, 197–198

Core values

acting on, 47

shared, 59

Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), 394–395

Corporations

in Gilded Age, 6

Council of Writing Program Administrators (WPA), 513

Counterfeit medicine, 117

Counters, 5

Court of Star Chamber, 127

Covert surveillance, 278–282

after September 11 attacks, 281–282

Carnivore system, 281

legislation authorizing, 282–285

Operation Shamrock, 280–281

wiretaps and bugs, 278–279

COVID-19

learning during, 113

lockdown, 1

remote work, 35, 477

Cox Communications survey, 141

CPAs (Certified Public Accountants), 416

Crash test dummies, gender bias, 436–437

Crawford, Sarah, 248

Creative Commons, 210–213

Credentials, 235, 242

Credit bureaus, 292–293

Credit cards

fraud, 136

privacy issues, 35

Credit reports, 248

Credit scoring, 392

Crime, computer

hackers. *See* Hacking

identity theft. *See* Identity theft

online predators, 137–138

Crito, 53

Cross-site scripting, 329

Crowdsourcing, 113

Cruise, Tom, 340

cryptocurrencies

features of, 115

financial concerns, 116–117

uses of, 115

Cuba and watch lists, 281

Cultural approach to technology, 37

Cultural relativism, 56–59

Customer service, monitoring, 481

Customs, 56

Cyber crime and cyber attacks, 334–336

denial-of-service, 334

incidents, 335–336

internet-of-things devices, 334

phishing and spear-phishing, 333

politically motivated, 337–341

SQL injection, 333

Cyber Sentinel program, 132

Cyberbullying, 141–142

Cybercafes, 114

Cyberlockers, 191

Cyberpunk: Outlaws and Hackers on the Computer Frontier, 325

D

Daily Telegraph, 255

Dalai Lama, 125, 338

DALL-E 2, 163

Danger Mouse (DJ), 187

Daoud, Ouhnane, 288

Darknets, 113

Dartmouth College, 13

Dartmouth Time-Sharing System (DTSS), 13

Data brokers, 248

Data-entry errors, 354–356

Data mining, 244

address books, 254–255

anonymized datasets, 251–252

cell phone tracking, 254

credit reports, 248

defined, 245–246

Facebook Beacon, 253–254

government, 293

household data, 253

Instagram terms of service, 255

IRS audits, 293–294

microtargeting, 249

opt-in and opt-out, 246–247

pregnant women, 247–248

profiling harms, 294

social network analysis, 249

Syndrome Surveillance System, 294

targeted direct mail, 248–249

telecommunications records database, 294

Data-processing systems, 8

Data-retrieval errors, 354–356

Databases

mining. *See* Data mining

regulation, 290–293

Davey Jones Locker, 174

Davies, Donald, 25

Davis, Jake, 341

Davis, Michael, 193

DDoS (distributed denial-of-service) attacks, 334, 335–338

de Colmar, Charles Thomas, 6

De George, Richar, 446

De Scandalis Magnatum law, 127

Declaration of Independence, 493

Deep Blue chess-playing program, 465

Deepfakes, 471–472

Deep learning, 466

Deezer music service, 197

Dehomag company, 9

Dell Computer, 477

Demographic parity, 395–396

DENDRAL, 465

Denial-of-service (DoS) attacks, 330, 333–334

Denning, Dorothy, 136

Denver International Airport, 363–364

Department of Agriculture, 356

Department of Defense

    COBOL programming language, 13

    TALON database, 282

Department of Health, Education, and Welfare, 291

Department of Justice

NCIC databases, 355–356

Depew, Chauncey, 21

Developing countries, text messaging in, 117

Development

professional and skills, 414–415

Diagnostic and Statistical Manual of Mental Disorders, 144

Diamond Multimedia Systems, Inc., 185

Diamond v. Diehr, 200

Dictionary attacks, 108, 316

Diebold voting machines problems, 365, 366

DIF (discriminant function), 294

DiFazio, William, 460

Difference Engine, 6

Difference principle, 83

Digital divide, 458, 487–488

critiques, 490–491

global, 488

models of technological diffusion, 489–490

net neutrality, 492–493

social, 489

Digital Due Process coalition, 284

Digital media, 187–188

Digital Millennium Copyright Act (DMCA), 188, 192

Digital rights management (DRM), 188–190

criticisms of, 189–190

online music stores, 190

Digital Telephony Act, 284

Digital video recorders (DVRs), 244

Digital watermark, 472

Direct mail advertising

costs, 253

targeted, 248

Direct recording voting machine failures, 364–367

Directory harvest attacks, 108

Disclosures, information. *See* Information disclosures

Discriminant function (DIF), 294–295

Disenfranchised voters, 354

Distributed denial-of-service (DDoS) attacks, 333, 335–336

Diversity, equity, and Inclusion, 435–436

Divine command theory, 59–62

Division fallacy, 527

DJ (Danger Mouse), 187

DMCA (Digital Millennium Copyright Act), 188

DNS (domain name service), 209

Do Not Call Registry, 302

Domain, public, 168

Domain name service (DNS), 209

Donald Duck, 176

Donations, 110

DoS (denial-of-service) attacks, 330, 333–334

DOS operating system, 18

Dot-com bust, 484, 498

Dotcom, Kim, 196

Downloads, drive-by, 329

Downsizing, corporate, 460

Doyon, Chris, 341

DRE system, 365

Drew, Lori, 142

Drew, Sarah, 142

Drive-by downloads, 329

Driver's licenses in Real ID Act, 297

DRM (digital rights management), 188–190

    criticisms of, 189–190

    online music stores, 190

Drones, 277

Drugs, pseudoephedrine purchases, 303

DTSS (Dartmouth Time-Sharing System), 13

Dudley Observatory, 6

Dula, Martin, 152

Dumpster diving, 136, 317

Dunn, Christopher, 275

Duties in Kantianism, 69

Dutifulness, 65

DVRs (digital video recorders), 244

E

E-ZPass system, 300–301

Earnest, Josh, 289

EarthLink service provider, 281

East Texas Cancer Center (ETCC), 370

Eavesdropping, 317

eBay, 253

Eckert, J. Presper, 9–10

Eckert-Mauchley Computer Corporation, 10–11

Economic inequality, 81–83

ECPA (Electronic Communications Privacy Act), 283, 318

Education in professional process, 414–416

EDVAC (Electronic Discrete Variable Automatic Computer), 9

EFF (Electronic Frontier Foundation)

fair use, 186

government request for email, 284

Egoism, ethical, 62–64

Egypt, 118

Eisenhower, Dwight, 11

Eldred, Eric, 176

Elections, U.S. Presidential

1896, 22

1952, 11

1984, 42

2000, 23, 354

Electricity, 18–19

Electromagnetism, 19–20

Electromagnets, 18–20

Electronic Communications Privacy Act (ECPA), 283, 318

Electronic Discrete Variable Automatic Computer (EDVAC), 9

Electronic Frontier Foundation (EFF)

fair use, 186

government request for email, 284

Electronic Numerical Integrator and Calculator (ENIAC) computer, 9–10, 12

Electronic Privacy Information Center (EPIC), 239, 303

Electronic waste (e-waste), 486–487

Elimination process, 521

Elitism, harmful effects of, 495–496

Email

ARPANET, 25

attachments, 324

government access to, 284

lost productivity from, 481

sexting, 135–136

spam. *See* Spam

Embedded computers, 35

Embedded system, 358

Emergent bias, 390

EMI agreement, 190

EMI publisher, 187

Employee monitoring, 481

Employee Polygraph Protection Act (EPPA), 270–271

Employer principles in Software Engineering Code of Ethics, 420–421

Employment. *See* Jobs

Encyclopedias, online, 113

Engelbart, Douglas, mother of all demos by, 31, 32

English language dominance, 494

Enhanced 911 services, 239

ENIAC (Electronic Numerical Integrator and Calculator) computer, 9–10, 12

Enlightenment, 125–126

Ennis, Ireland, 490–491

Enquire program, 33

Entertainment, digitized, 34–35

EPIC (Electronic Privacy Information Center), 239, 303

Epic Games, 271

EPPA (Employee Polygraph Protection Act), 270–271

Equality of opportunity, 396

Equalized odds, 396

Equifax credit reporting agency, 253, 292–293

Errors

    data-entry and data-retrieval, 354–356

    software and billing, 356–358

Espionage, 340

eSports, 106

Esposito, Dawn, 460

Estonia

    cyber attacks in, 337

Estrada, Joseph, 118

Ethernet, creation of, 31

Ethical egoism, 62–64

Ethics, 47–48

definitions, 48–49

discussion questions, 99–101

in-class exercises, 101–102

law breaking, 93–96

professional. *See* Professional ethics

review questions, 98–99

scenarios, 50–53

theories, 53–54

act utilitarianism, 70–75

comparing, 92

cultural relativism, 56–59

divine command theory, 59–62

ethical egoism, 62–64

Kantianism, 64–70

rule utilitarianism, 75–79

social contract theory, 79–86

subjective relativism, 54–56

virtue ethics, 86–92

Ethiopian Airlines Flight 302, 386–387

European farm lobby, 484

European Union survey, 324

Evans, Josh, 142

Exiled Tibetan government, cyber attacks in, 338

Exit polling, 24

Experian credit reporting agency, 249, 253, 292–293

Extended Copy Protection, 189

F

Facebook, 250

Arab Spring uprisings, 118

HTTPS option, 321

KLM seatmate program, 112

privacy, 227–228

tags, 238–239

Facebook Beacon, 253–254

Facebook Login, 242

Facebook's algorithms, 121

Facial recognition software, 239, 276

Faggin, Federico, 14

Fair and Accurate Credit Transactions Act, 293

Fair Credit Reporting Act, 292–293

Fair use, 181–182

Audio Home Recording Act, 184

books, 186–187

and DRM, 189–190

examples, 182–183

mashups, 187

space shifting, 185–186

thumbnail photographs, 185–186

time shifting, 183

Fairchild Semiconductor, 13–14

Fairness, definitions of, 395–397

FairPlay system, 190, 197

Fake reviews, 137

Fall Joint Computer Conference, 31

Fallacies

affirming the consequent, 524–525

bandwagon fallacy, 526–527

begging the question, 525–526

denying the antecedent, 525

division fallacy, 527

of equivocation, 527–528

faulty generalization, 527

slippery slope argument claims, 526

Fallacy of equivocation, 527–528

Fallon, Jimmy, 163

False arrests, 354–356

False Claims Act, 444

False information in networking, 140–141

Falun Gong, 125

Fandango, 253

Faris, Iyman, 282

Farm lobby, 484

Farnsworth, Philo, 23

Faulty generalization, 527

FBI. (Federal Bureau of Investigation), 319

    CALEA, 284

    Carnivore surveillance system, 281

    identity theft investigations, 136

    Mayfield detention, 288–289

    NCIC, 272–274, 354

    Patriot Act, 285–286

    secret wiretapping, 279

FCC (Federal Communications Commission)

    CALEA guidelines, 284–284

    and First Amendment, 128–129

loud television commercials, 302–303

FCC v. Pacifica Foundation et al., 128

FDA (Food and Drug Administration), 371

Federal Aviation Administration, 277

Federal Bureau of Investigation (FBI), 319

CALEA, 284

Carnivore surveillance system, 281

identity theft investigations, 136

Mayfield detention, 288–289

NCIC, 272–274, 354

Patriot Act, 285–286

secret wiretapping, 279

Federal Communications Act, 279, 283

Federal Communications Commission (FCC)

CALEA guidelines, 284–285

and First Amendment, 128–129

loud television commercials, 302–303

Federal Education Rights and Privacy Act (FERPA), 299

Federal Trade Commission (FTC)

Facebook complaint, 239–240

Open Internet Order, 492

telemarketing, 302

Feinstein, Diane, 289

Felten, Edward, 189

FERPA (Federal Education Rights and Privacy Act), 299

Ferranti Mark 1 computer, 33

File-hosting services, 191

File sharing on peer-to-peer networks. *See* Peer-to-peer networks

Filters

collaborative, 245

spam, 107–108

web, 132

"Filthy Words" monologue, 128–129

Final Rip Off, The, 107

Financial Services Modernization Act, 293

fingerd program, 326, 327

Fingerprint misidentification, 288

Fire alarm telegraphs, 20

Firefox web browser, 33, 209, 214

Firesheep browser case study, 320–322

Firewalls, 342

First Amendment to the U.S. Constitution

    history of, 127–129

    limitations, 128

FISA (Foreign Intelligence Surveillance Act), 283

FISC (Foreign Intelligence Surveillance Court), 289

Flash cookies, 244

Flickr site, 113

Florida, voting machine errors, 364–367

FLOW-MATIC programming language, 12–13

Floyd, George, 119

Folkways, 56

Fonda, Jane, 281

Food and Drug Administration (FDA), 371

Ford, Gary, 414

Ford Motor Company, 447–448

Foreign Intelligence Surveillance Act (FISA), 283

Foreign Intelligence Surveillance Court (FISC), 289

Foreign workers, 485–486

FORTRAN programming language, 12

Fountainhead, The, 62

Fourth Amendment to the U.S. Constitution

    AIT scanners, 303

    and electronic surveillance, 278–282

    and Patriot Act, 285–286

Fourteenth Amendment to the U.S.Constitution, 447

Foxconn, 36

Framingham Heart Study, 64

France, privacy laws, 291

Frank, Robert, 493–496, 498

Franklin, Benjamin, 168, 216

Franklin ACE computer, 198

Frankston, Bob, 17

Fraud, credit card, 136

Free press, 30

Free riders, 84

Free trade agreements, 483

Freedom High School, 135

Freedom of expression, 127–128

    ethical evaluations, 133–134

    FCC v. Pacifica Foundation et al., 128–129

    history, 127–128

    limitations, 128

    Mill on, 126

Freedom of Information Act, 300

Freelance Hellraiser, 187

Friedman, Batya, 389

Friends of the Earth, 484

FTC (Federal Trade Commission)

Facebook complaint, 238–239

Open Internet Order, 492

telemarketing, 302

ftp application, 326

Fundamentals of Engineering (FE) exam, 417

G

Gaines, Homer, 261

Galilei, Galileo, 122–123

Game of Thrones, 34–35

Games, online, 114, 147

GAO (General Accounting Office), 359

Garner, Amanda, 357

Gates, Bill, 16, 485

GDPR (General Data Protection Regulation), 244

Gender bias, 436–437

General Accounting Office (GAO), 359

General Data Protection Regulation (GDPR), 244

General Electric, software development teams in India, 482

Generative AI, 467

Generic trademarks, 171

Genesis, 62

Genetic Information Nondiscrimination Act, 271

"Genie in a Bottle," 187

Georgia, Republic of, 337

Germany

    personal data collection, 413

    privacy laws, 291

    revenge porn, 142

    Web censorship, 125

Gershwin Publishing Corporation v. Columbia Artists Management, Inc., 174, 194

Gert, Bernard, 78

Gertner, Nancy, 193

Get Creative, 210–211

GhostNet system, 338

Gibbs, Norman E., 414

Gig economy, 479–481

Gilded Age, 6

Glaucon, 101

Glidden, Carlos, 22

Global divide, 488

Global Science Research, 256

Globalization, 482

    arguments against, 484

    arguments for, 483

    international competition, 486

    multinational teams, 482

Gmail, Blue Frog bot for, 335

GNU Project, 209

GNU Public License, 209

Gold farmers, 114

Golden Rule, 100

Gonzalez, Albert, 336

Good vs. God, 61

Good will in Kantianism, 65–67

Goodearl, Margaret, 443

Google

- fair use case, 186–187
- government request for email, 284
- information storage by, 285
- Oracle, 199
- revenge porn, 142
- smartphone patent wars, 202

Google Maps, 242

Google Photos, 390

Google Privacy Checkup, 254

Google search engine

pages indexed, 34

personalized search, 245

rankings in, 141

tiered services opposition, 492

Gore, Al

Florida vote count, 23

on surveillance, 289

Govern, Maureen, 252

Government, 269

censorship through, 122–123

census records, 271–272

closed-circuit television cameras, 275–276

covert government surveillance, 278–282

data mining, 293–295

database regulation, 290–293

discussion questions, 307–308

in-class exercises, 308

information collection by, 270–277

information collection legislation, 270
information dissemination, 298–302
invasion, 302–305
IRS records, 272
license plate scanners, 276
national ID cards, 295–298
NCIC database, 272–274
Patriot Act, 285–290
review questions, 306
and virtue ethics, 91
wiretapping legislation, 282–285
GPS, OnStar, 242
Gramm-Leach-Bliley Act, 293
Graphical user interfaces, 31–32
Grassley, Chuck, 307
Great Britain, surveillance cameras in, 275
Great Firewall of China, 125

Greatest Happiness Principle, 73

Greek alphabet, 28

Green Stamps, 239

Greenpeace, 484

Greensboro, N.C.sit-ins, 85

Grey Album, The, 187

Grills, Ashley, 142

Grocery club cards, 240

Grokster network, 191–193

Guardian, 283, 289

Guide software, 32

Guilford County voting machine errors, 366

Gulf War, 359

Gutenberg, Johannes, 29

Gutenberg Bible, 29

Guzner, Dmitriy, 341

Gyges, legend of, 101

H

H-1B visas, 485–486

“Hack SDMI” challenge, 189

Hacking

    FBI and Locked iPhone, 319

    Firesheep case study, 320–322

    incidents, 318

    penalties for, 318

Hacktivists, 340

Hafner, Katie, 325

Hallucination, 470

Hamlet scenario, 166–167

Hanger, Charles, 273

“Happy Birthday to You,” 170

“Hard to Explain,” 187

Harmonic telegraph, 21

Harris Interactive study, 302

Harrison, George, 199

Harvard Law Review, 231–232

Harvard University, admissions software for, 318–319

Hasty generalization, 527

HAVA (Help America Vote Act), 364–365

Health care, 3, 80

Health Information Technology for Economic and Clinical Health (HITECH) Act, 243

Health Insurance Portability and Accountability Act (HIPAA), 300

Help America Vote Act (HAVA), 364–365

Henry, Jalani, 269

Henry, Joseph, 19

Henry, Patrick, 127

Hernandez, Roberto, 354

Hertz, Heinrich, 22

Herzenberg, Joe, 261

"He's So Fine," 199

Hewlett Packard, 482

HIPAA (Health Insurance Portability and Accountability Act), 300

History

computing. *See* Computing milestones

information storage and retrieval. *See* Information storage and retrieval milestones

networking. *See* Networking

HITECH (Health Information Technology for Economic and Clinical Health) Act, 243

Hitler, Adolf, 9

Hobbes, Thomas, 79

Hoff, Marcian "Ted," 14

Holberton, Frances, 12

Hollerith, Herman, 8

Holocaust, 9, 140

Homebrew Computer Club, 15–18

Homophily, 435

Hoover, J. Edgar, 273

Hopper, Grace Murray, 12

Horca, Joahnna, 457

Horne, Thomas, 135

Hostile work environments, 437

Hosts for viruses, 322

Hotmail, Blue Frog bot for, 335

Hotspots, 27

HTC in smartphone patent wars, 202

HTTP (HyperText Transport Protocol), 320

Hughes Aircraft case, 442–444

Hulu Plus video service, 197

Humanitarian action, online, 114

Hursti, Harri, 366

Hussein, Saddam, overthrow of looting after, 79

self-censorship after, 124

Hybrid computer chips, 442–443

Hybrid work, 479

HyperCard system, 32

Hypertext systems

evolution of, 30

networked. *See* World Wide Web (WWW)

single-computer, 32–33

HyperText Transport Protocol (HTTP), 320

Hypothetical social contract agreements, 85

I

Ibarra, Ruth, 443

IBM (International Business Machines)

BIOS, 199

Chinese acquisition of assets, 486

early success, 12

formation of, 8

higher-level programming languages, 12

Holocaust role, 9

IBM PC computers, 17

System/360 computers, 14

iCow service, 117

Identification cards, national, 295–298

Identity theft law for, 293

national ID cards, 295–298

overview, 136–137

Real ID Act, 297–298

Identity Theft and Assumption Act, 136

Identity Theft and Assumption Deterrence Act, 318

Identity Theft Penalty Enhancement Act, 136

IEEE-USA, 417

Immigration and Naturalization Service, 318

IMP (Interface Message Processor), 25

Impact Pro, 391

Imperfect duties, 69

Implanted chips, 242

Inclusive language and behavior, 438

Income tax, 272

India
direct recording voting machines, 364, 365
globalization of jobs to, 486
IT development in, 486
for multinational teams, 482
Inequality, economic and social, 81–83
Information Age, catalysts for, 1
Information collection
by government, 271–277
legislation, 270
in privacy, 269–270
Information disclosures
automobile black boxes, 243
body scanners, 240–241
cookies, 244
digital video recorders, 244
enhanced 911 services, 239
Facebook tags, 238–239

implanted chips, 242

medical records, 243–244

mobile apps, 242

OnStar system, 242–243

private organizations, held by, 237–238

public records, 237

rewards programs, 239–240

RFIDs, 241–242

Information dissemination, 270, 298–302

Information Hiding Workshop, 189

Information processing in privacy, 270, 290

Information storage and retrieval milestones

codex, 29

graphical user interfaces, 31–32

Greek alphabet, 28

hypertext, 30

newspapers, 30

printing press, 29

search engines, 34

World Wide Web, 33

Information technology (IT)

declining costs, 482

digital divide, 487–493

dot-com bust, 484–485, 498

history

computing. *See* Computing milestones

information storage and retrieval. *See* Information storage and retrieval milestones

networking. *See* Networking issues, 34–36

Iniguez, Noe, 143

Innovation commons, 211

Inquisition, 122–123

Instacart company, 479

Instagram terms of service, 255

Instant messaging

popularity, 137
Instant photography patents, 173
Instrumentalism, 36
Integrated circuits, 13
Intel Corporation, 485
4004 microprocessor, 14
founding of, 14
India offices, 482
software growth encouraged by, 205
stock price, 484
Intellectual activities, privacy for, 230
Intellectual property
Apple/EMI agreement, 190
Creative Commons, 210–213
digital rights management, 188–190
DMCA, 188
Extended Copy Protection, 189
fair use, 181–187

in-class exercises, 217
open-source movement, 206–210
peer-to-peer networks, 191–196
protection of
    benefits, 168
    case study, 177–181
    copyrights, 173–176
    limitations, 168–170
    patents, 171–173
    trade secrets, 170–171
    trademarks and service marks, 171
SDMI, 188
    software protection, 197
    copyrights, 197–198
    legitimacy of, 203–206
    patents, 200–203
    safe development, 199–200
Xbox One, 190–191

Intellectual virtues, 86–87

Interest-free loans, 114

Interface Message Processor (IMP), 25

Internal Revenue Service (IRS)

audits, 293–294

data collection, 272

Privacy Act of 1974, 291–292

Social Security number requirement, 295–296

International Business Machines (IBM)

BIOS, 199

Chinese acquisition of assets, 486

early success, 12

formation of, 8

higher-level programming languages, 12

Holocaust role, 9

IBM PC computers, 17

System/360 computers, 14

International Collegiate

Programming Contest, 486

International competition, 486

International Data Corporation survey, 481

International Federation of the Phonographic Industry, 195

International Olympic Committee, 125

Internet, 25–26, 111

addiction to

contributing factors, 145

ethical evaluation, 145

reality of, 143, 144

apps, 112

Carnivore surveillance system, 281

censorship on, 126

controlling, 124–125

global divide, 488–489

music services, 197

net neutrality, 492–493

networking. *See* Networking

uses, 112–114

World Wide Web, 111–112

Internet-connected devices, 331

Internet control, 124

Internet Explorer browser, 33

Internet of Things, 114

Internet-of-Things (IoT) devices, 334

Internet Protocol (IP), 26

Internet radio, 188

Internet Research Agency (IRA), 120–121

Internet worm, 325–329

Internment camps, 272–273

Intimacy and privacy, 230

Invasion of privacy, 302–304

IP (Internet Protocol), 25

iPAQ handheld computer, 358

iPhone, 319

address book uploads, 254–255
Iran, 339–340
Iraq War
looting in, 79
self-censorship in, 124
Ireland, 490
IRS (Internal Revenue Service)
audits, 293–294
data collection, 272–273
Operation Shamrock, 280–281
Privacy Act of 1974, 291–292
Social Security number requirement, 295–296
Is Anyone Up? site, 142
Isaac, 62
Islam, 59
IT (Information technology)
declining costs, 482
digital divide, 487–493

dot-com bust, 484–485, 498

history computing. *See* Computing milestones

information storage and retrieval. *See* Information storage and retrieval milestones

networking. *See* Networking issues, 34–36

ITT Communications, 280

iTunes Music store, 190, 197

J

J-Com company, 364

Jackson, Sheila, 397

Jackson, Shirley, 397

Janesch, Rachel, 443

January 6, 2021, Events of, 119

Japan, air traffic control system failure, 357

Japanese-American internment, 272–273

Jay Z, 187

Jeep Cherokee, 357

Jennings, Christine, 366

Jennings, Ken, 465, 466

Jeopardy! television program, 465–466

Jerome- Parks, Scott, 374

Jet Propulsion Laboratory, 362

Jn-Charles, Alexandra, 374

Jobs

automation effects

jobs gained from, 461–462

jobs lost from, 458–460

productivity changes from, 462–463

supply-chain, 477

background checks, 238

discussion questions, 500–502

gender bias, 436–437

gig economy, 479–481

global movement, 482–487

in-class exercises, 502–503

monitoring, 481

multinational teams, 482

organization changes, 476–477

review questions, 499

temporary work, 479

vacations, 463–464

Jobs, Steve, 15, 16, 31

Johnson, Lyndon, 300

Johnson & Johnson, 171

Jonson, Ben, in *Hamlet* scenario, 166

Jordan, Eason, 123

Judaism, 59

Judgment principles in Software Engineering Code of Ethics, 422

Just deserts argument, 204

Just-in-time production, 477

Juvenal, 122–123

K

Kahn, Robert, 25

Kant, Immanuel

on addiction, 145

beliefs, 65

on censorship, 125

on duties, 81

Kantianism, 64

case against, 69–70

case for, 68–69

ethical evaluations

canceled vacation, 463–464

CIPA, 133

Firesheep case, 322

intellectual property, 178

Internet addiction, 145

Internet worm, 328–329

privacy, 236

scenario for, 67–68

sting operation, 138–139

good will and Categorical

Imperative in, 65–67

law breaking in, 93–94

Kapauku of Papua, 462

Katz, Charles, 280

Kay, Alan, 31

Kaysen, Carl, 290

Kazaa network, 191–193

Ke Jie, 466, 467

Kelly, Leslie, 185–186

Kelly, Max, 338

Kelly v. Arriba Soft Corporation, 185–186

Kemeny, John, 13

Kenadek, Richard, 174

Kennedy, Robert, 280, 282

Kennestone Regional Oncology Center, 368

Kepler, Johannes, 5

Kerry, John, 366

Kik messenger, 137

Kilby, Jack, 14

Kilminster, Joe, 442

Kimball, Curtis, 118

Kimberly-Clark, 171

King, Martin Luther, Jr., 273, 281

King for a Day, 170

Kiva site, 114

Kleenex brand, 171

Kleinrock, Leonard, 25

Kling, Rob, 491

KLM airline, 112

Knight Capital, 353

Knowledge economy, 458

Knuth, Donald, 210

Kodak, 173

Kogan, Aleksandr, 256, 257

Kolata, Gina, 325

Krum, Charles and Howard, 22

Kung Bushmen, 462

Kurtz, Thomas, 13

Kyl, Jon, 307

L

L-1 visas, 485–486

Ladder of privacy, 230

Lafferty, Dan, 465

LaMacchia, David, 174–175

Land, Edwin, 173

Lane, Sean, 253

LaPorte voting machine errors, 366

Large language models, 252

LaRue, Donald, 443

Laws

breaking, 93–96

act utilitarianism, 96

conclusion, 96

Kantianism, 94–95

rule utilitarianism, 95–96

social contract theory, 94

Robotics, 458

for winner-take-all effects, 495–496

Leahy, Patrick, 307

Learning, online, 113

Lea, Elina, 187

Legal online access to entertainment, 197

Legal responsibility, 447

Legislation. *See* Government

Lei, Hong, 340

Leibniz, Gottfried, 6

Leiner, Barry M., 25

Lenovo company, 486

Lentz, Jacobus, 413–414

Leonard, Andrew, 210

Lessig, Lawrence, 169, 211

Letters, National Security Letters, 286–287

Leveson, Nancy, 372–373

Leviathan, 79

Leviticus, 59

Libel laws, 127

Libya, 118

License plate scanners, 276

Licensing, 415

    Creative Commons, 211–213

    direct censorship through, 123

    inventions, 173

    open-source software, 207

    software engineers, 417

software patents, 200, 201

Licensing Act, 30

Licklider, J.C.R., 25

Lie-detectors, 270

Lightner, Lisa, 443

Limbaugh, Rush, 243

Limited rights, 81

Lindh, JohnWalker, 288

Linear accelerators. *See* Therac-25 linear accelerator

LinkedIn, 112

Linspire, 195

Linux

impact, 210

in open-source movement, 210

Lion Air Flight 610, 384–386

Lisa computer, 31

Live Free or Die Hard, 315

LiveSecurityWatch, 235

Loan applications, 35

Loans, 114

Locke, John, 80, 164–165, 174, 204

Locked iPhone, 319

Lockheed Martin, 362

Logan, Jesse, 135

Logarithms, 5

Logography, 28

London dispatch system failure, 357

Long-distance telephone systems, 361

Los Angeles County+ USC Medical Center, 357

Lotus Development Corporation, 253

Loud television commercials, 302–303

Loyalty programs, 239

Lun, Cai, 29

Lund, Robert, 442

Lundström, Carl, 196

Luther, Martin, 29

Luxury taxes, 496

Lyft company, 480

M

M-PESA services, 105, 117

Macedonia, 105

Macedonian Entrepreneurs, 120

Machine-learning algorithms, 390

Macintosh computers, 31

Madison, James, 128

Mail

email. *See* Email

targeted direct, 248–249

Mainframe computers, 14

Major League Baseball, 481

Malaysia Airlines, 357

Malls, cell phone tracking in, 254

Malware, 322
Backdoor Trojans, 329
bots and botnets, 330–331
cross-site scripting, 329
drive-by downloads, 329
Ransomware, 329–330
rootkits, 330
security risks, 332
spyware and adware, 330
Trojan horses, 329
viruses, 323–325
worms
Internet, 325–329
types, 325–329
Management principles in Software Engineering Code of Ethics, 423
Mandiant company, 340

Maneuvering Characteristics Augmentation System (MCAS), 382–383

Many/any fallacy, 58

Maps, Google Maps, 227, 242

Marconi, Guglielmo, 22

Marconi Wireless Telegraph Company, 22–23

“Marketplace: Households” CD, 253

Markoff, John, 325, 327

Mars missions, 362

Marshall Field’s, 8

Mashups, 187

Mason, George, 127

Mason, Jerald, 442

Massachusetts Institute of Technology admissions software for, 318

MasterCard Operation Payback attack, 341

Mattrick, Don, 191

Mauchly, John W., 9–10

Maxwell, James Clerk, 22

May, Christopher, 188

Mayfield, Brandon, 288–289, 308

Mazor, Stanley, 14

McAuliffe, Christa, 441

McFarland, Michael, 448

McGinn, Mike, 277

McGuire, Melanie, 301

McKinley, William, 22

McLeod, Kembrew, 169

McNealy, Scott, 227

McNerney, Jim, 381

McVeigh, Timothy, 272–274

Mechanical calculators, 6–7

Media Player, 190

Medical records, 243–244

Medicine, counterfeit, 117

Medick company, 403

Megan Meier Cyberbullying Prevention Act, 142

Megaupload Limited, 196, 341

Meier, Megan, 141, 142

Memex system, 30

Memory in EDVAC, 9

Mental condition for moral responsibility, 374

Merchandise 7X formula, 170

Mercury Theater, 23

Merit Systems Protection Board, 444

Mestas, Colleen, 243

Methamphetamine, 303

Mettenbrink, Brian, 341

MGM *v. Grokster*, 193–194

Miceli, Marcia, 444

Microlending, 114

Microprocessors

- invention, 14–15
- uses, 14

Microsoft Corporation
BASIC interpreter, 16
ClearType technology, 173
DOS, 18
India offices, 482
information storage, 284
patent applications, 200
smartphone patent wars, 202
and software piracy, 204–205
stock prices, 484–485
Windows systems, 31
Xbox One, 190–191
Microtargeting, 249
Microwave radar systems, 13–14
Middlemen, eliminating, 477, 497
Milestones
computing. *See* Computing milestones
information storage and retrieval.

See Information storage and retrieval milestones

networking. *See* Networking

Mill, John Stuart

and act utilitarianism, 70

on censorship, 125–126

on pleasures, 145

on Principle of Harm, 126–127

and rule utilitarianism, 75

Mining, data. *See* Data mining

Minuteman II ballistic missiles, 14

Missile system failures, 359–360

Missiles, 14

Misuse of sources, 514

Mitnick, Kevin, 316

MITS company, 16

Mizuho Securities, 364

Mobile apps, 112, 242

Mocmex Trojan horse, 329

Models

of technological diffusion, 489–490

Modus ponens, 520–521

Modus tollens, 521

Mondale, Walter, 42

Monitoring in workplace, 481

Monks, 29

Monmouth University poll, 277

Montclair State University, 149

Monty Python's Flying Circus, 107

Moon landings

faked, 140

transmission of, 23

Moore, Gordon, 14

Moore, Hunter, 142

Moore School, 9

Moore's Law, 14

Moral capital, privacy as, 230

Moral luck problem, 75

Moral responsibilities

characteristics, 440–441

conditions for, 388–389

Moral virtues, 86–88

Morality *vs.* ethics, 48–49

Moravec, Hans, 465–467

Morin, David, 254–255

Morris, Robert Tappan, Jr., 325–329

Morse, Samuel, 18, 20

Morse code, 21

Morton Thiokol, 442

Motion Picture Association of America (MPAA)

copyright extension support, 175

Operation Payback attack, 341

Motorola

cell phones, 27

smartphone patent wars, 202

Mouse, invention of, 31

MoveOn.org, 253

MP3 music files, 188

MPAA (Motion Picture Association of America)

copyright extension support, 175

Operation Payback attack, 341

Multifactor authentication, 317–318

Multinational teams, 482

Muris, Timothy, 302

Murphy, Eddie, 170

Murrah, Alfred P., 273

Murrah Federal Building bombing, 273

Music

legal Internet services, 197

mashups, 187–188

piracy, 187

Musical telegraph, 21

Muslims, 59

"My Sweet Lord," 199

MYCIN, 465

Myst game, 33

N

Nachi worm, 76, 77

Nader, Ralph, 484

NAFTA (North American Free Trade Agreement), 483

Napier, John, 5

Napster network, 191–193

Nardone v. United States, 279

NASA

- Mars missions, 362
- Space Shuttle disaster, 441–442

NASDAQ stock exchange, 357

Nashi group, 337

National Archives, 113

National Bureau of Standards, 10

National Council of Examiners for Engineering and Surveying (NCEES), 417

National Crime Information Center (NCIC), 272–274, 354–356

National Data Center, 291

National Data Exchange (N-DEx), 274–275

National Do Not Call Registry, 302

National Fraud Alert System, 293

National Highway Traffic Safety Administration, 357

National ID cards, 295–298

National Organization of Women, 132

National Security Agency (NSA)

- Internet access, 283
- phone record access, 289–290
- telecommunications record database, 294
- watch lists, 281
- wiretapping, 280–281

National Security Letters, 286–287

National Stolen Property Act, 318

Natural rights

    privacy, 231–234

    software protection, 203–204

Nautical Almanac Office, 6

Nazi government, 9, 413

NCIC (National Crime Information Center), 272–274, 354

Near, Janet, 444–443

Negative rights, 80

Neij, Fredrik, 196

Nelson, Ted, 30

Net Addiction Treatment Center, 114

Net neutrality, 492–493

Netflix video service, 163, 197

    movie rating prize, 251

Netflix video service net neutrality, 492

Networked hypertext systems. *See* World Wide Web (WWW)

Networking, 105–106

addiction to, 143–145

censorship in, 122–127

and children, 131–135

cyberbullying, 141–143

fake reviews, 137

false information, 140–141

freedom of expression, 127–131

identity theft from, 136–137

in-class exercises, 152–153

Internet, 112–114

Internet Research Agency, 120–121

Macedonian Entrepreneurs, 120

milestones, 18

ARPANET, 25

broadband, 27

electricity and electromagnetism, 18
email, 25
Internet, 25
NSFNET, 27
online predators, 137–138
radio, 22–23
remote computing, 24
telegraph, 20
telephone, 20–22
television, 23–24
typewriters and teletypes, 22
wireless, 27
peer-to-peer, 191–197
political activism, 118
revenge porn, 142
spam, 107–111
text messaging, 117
traditional newspapers, 121–122

Neumann, Peter, 397

Neutrality thesis, 36

New Technologies Products (NTP), 201

New York City, surveillance cameras, 275

New York City Housing Authority, 356

New York Civil Liberties Union (NYCLU), 275

New York Stock Exchange, 338, 357

News agencies, self-censorship by, 123

Newspapers, 30, 121–122

NeXT computer, 33

Nicomachean Ethics, The, 86

Nipkow, Paul, 23

Nissenbaum, Helen, 389

Nix, Alexander, 256

Nixon, Richard

    war on drugs, 281

NLS system, 31

No Electronic Theft Act, 174–175

Nokia in smartphone patent wars, 202

Non-fungible token (NFT), 176–177

Nonhistorical social contract agreements, 85

Nonpolitical speech, freedom of, 128

Normalization model, 490

Norms, 55–56

Norris, Pippa, 498

North American Free Trade Agreement (NAFTA), 483

North Korea, Internet access in, 124

Noyce, Robert, 13, 14

Nozick, Robert, 204

NSA (National Security Agency)

- Internet access, 283
- phone record access, 289–290
- telecommunications record database, 294
- watch lists, 281
- wiretapping, 281–282

NSFNET, 27

Nuclear power plants, 3

Nugent, Alan, 344

O

Obama, Barack

CALM Act, 302–303

NSA phone record access, 289

PRISM program, 283

Objectivism, 92

Oei, Ting-Yi, 135

Oersted, Christian, 18

Office of the Inspector General, 443

Office Workstations, Ltd., 32

Oklahoma City bombing, 273

Olean, NY, surveillance cameras in, 275

Olmstead, Roy, 278–279

Olmstead v. United States, 278–279

Olson, Theodore, 132

Olympics, 125

Omnibus Crime Control and Safe Streets Act, 283

Online communities, 22

Online courses, 491–492

Online predators, 137–138

Online System, 31

OnStar Corporation, 242–243

Ontario Cancer Foundation, 369

Open and closed platform, 207

Open64 compiler, 486

Open Internet Order, 492

"Open Letter to Hobbyists, An," 16

Open platform, 207

Open Source Initiative, 12

Open-source software, 206

    benefits, 208

    definition, 208

    examples of, 209

GNU Project and Linux, 209–210

impact, 210

vs. proprietary, 203–204

Open Voting Consortium, 367

OpenOffice.org, 209

Operation In Our Sites, 196

Operation Payback, 341

Operation Shamrock, 280–281

Opsahl, Kurt, 252

Opt-in policies, 246–247

Opt-out policies, 246–247

Optimists, technological, 490

Oracle company, 482

Oracle program, 326

Oracle v. Google, 199

Ordeals, 235

Organization changes in workplace, 476–477

Organized crime, 280

Overgrazing problem, 84

Ovid, 122–123

Oxfam, 484

P

Pacific Research Institute, 367

Pacifica Foundation, 129

Packet-switched networking, 26

Palo Alto Research Center (PARC), 31

PalTalk, NSA access to, 283

Pandora music service, 197

Paper, invention of, 29

Paper audit trails, 366, 398

Papert, Seymour, 38

Papua, 462

Papyrus scrolls, 29

Paradoxes, intellectual property, 165

Paramount Pictures, 170

PARC (Palo Alto Research Center), 31

Parchment, 29

Party phone lines, 22

Pascal, Blaise, 6

Password guidelines, 316–318

Patent and Trademark Office, 200

Patent-holding companies, 201

Patent trolls, 200, 201

Patents

    purpose, 171–173

    software, 200–203

Paterson, William, 282

Path Intelligence, 254

Path site, 254–255

Patriot Act, 285

    National Security Letters, 286–287

    NSA access to phone records, 289

principal limitations, 292

provisions, 285–286

responses, 287–288

successes and failures, 288–289

Patriot missile system failures, 359, 360

Pay ratios, CEOs to production worker, 494

PayPal service

Operation Payback attack, 335, 341

phishing, 136

PC bangs, 114

Peele, Stanton, 145

Peer-to-peer networks, 191

BitTorrent, 194–195

Internet music services, 197

Megaupload Limited, 196

MGM v. Grokster, 193–194

Pirate Bay, 195–196

PRO-IP Act, 196

Pen registers, 293

Pennsylvania Steel Company, 8

Pentagon, terrorist attack on, 285

People's Computer Center, 16

People's Computer Company, 15

People's Liberation Army, 340

People's Republic of China dictatorships, 484

    IBM assets acquired by, 486

    Internet access, 124–125

Perfect duties, 69–70

Perl language, 209

Persistent online games, 150–151

Personal computers

    graphical user interfaces, 31–32

    invention of, 16–18

Personal information, 238

Personalized search, 245

Persuasive essays, 530

Pessimists, technological, 490

Pew Internet & American Life Project, 192

Pew Surveys, 489

PGA Tour, 495

PharmaMaster spammer, 335–336

Philippines, 118

Phishing, 136, 333

Photographs

    copyrights, 185–186

    sexting, 134–135

Photoshop trademark, 171

PHP language, 209

Pinto, Ford, 448

Piracy, 197

Pirate Bay site, 195–196

Pistole, John, 303

Plagiarism

    avoiding, 514

citing sources, 514

consequences, 513

misuse of sources, 514

types, 513–514

Plato

Crito, 53

Republic, The, 101

Player Piano, 458

PlayStation 4, 191

Plowman, James, 135

Polaroid Corporation, 173

Police

social network monitoring, 249–250

sting operations, 138–140

Police drones, 277

Political content

blocking, 125

text messaging for, 118

Politically motivated cyber attacks, 337–342

Polygraphs, 270–271

Pony Express, 20–21

Poor and rich, growing gap between, 490

Pornography

blocking, 125

child, 135

child pornography scenario, 430–431

revenge, 142–143

Sesame Street channel hacking, 319

Web filters for, 132

Portland Seven, 288–289

Positive rights, 80

Possessions *vs*. time, 462–463

Postal Inspection Service, 137

Postal Service, 356

Potter, Stewart, 280

Pragmatism, 37

Predators, online, 137–138

Predictive policing, 392–394

Preexisting bias, 390

Pregnant customers, data mining targeting of, 247–248

Premises

backing, 518

grounds, 518

types, 518

warrant, 518

Prepublication reviews, 123

Presidential elections, U.S.

1896, 22

1952, 11

1984, 42

2000, 23, 364

Principle of Harm, 126–127

Principle of Utility, 70–71, 75

Principles of justice, 81–83

Printing press, 29, 123

Prior restraints on expression, 127

Prioritization Resources and Organization for Intellectual Property (PRO-IP) Act, 196

PRISM program, 283

Privacy, 35, 227–228

for autonomous moral agents, 234

benefits, 229–230

case study, 235–237

data mining, 244–251

definition, 228–229

DRM effect, 190

government actions. See Government

harms, 229

historical evolution, 235–236

in-class exercises, 261–262

information disclosures, 237–244

ladder of, 230

natural right to, 231–234

Privacy (*Continued*)

as prudential right, 234

rights associated with, 232–233

and telemarketing, 302

and telephones, 21–22

Privacy Act of, 1974, 291–292, 355

Private organizations, information held by, 237–238

PRO- IP (Prioritization Resources and Organization for Intellectual Property) Act, 196

Problem of moral luck, 75

Procter & Gamble, 238

Product principles in Software Engineering Code of Ethics, 421–422

Production workers, pay ratios to CEOs, 494

Productivity

from automation, 461

changes in, 461

monitoring, 481

Profession principles in Software Engineering Code of Ethics, 423–424

Professional development, 415

Professional ethics, 413–414

case studies, 428

antiworm, 431–433

child pornography, 430–431

consulting opportunity, 433–435

software recommendation, 429–430

discussion questions, 450–452

in-class exercises, 453–454

review questions, 450

software engineering. *See* Software Engineering Code of Ethics and Professional Practice

whistle-blowing, 440–441

Hughes Aircraft case, 442–444
legislation, 444
morality of, 444–448
Morton Thiokol case, 441–442
and organizational failure, 445–446
Professional societies, 415
Professions
characteristics, 414–416
computer-related, 416–418
CPAs, 416
definition, 414–415
Profiling harms, 294–295
Programming languages early, 12–13
Promenade Temecula mall, 254
Proof-of-stake protocol, 116
Proof-of-work protocol, 115
Property
intellectual. *See* Intellectual property

natural right to, 164–165

Propositions of argument

conclusion, 518

premises, 518

variable, 518

Proprietary software, 203

Protect America Act, 283

Protestant Reformation, 29

Prudential rights, 234

Pseudoephedrine purchases, 303

Psychographic profiles, 255–256

Public access wireless networks, 27–28

Public domain, 168–169

Public information. *See* Information disclosures

Public life *vs*. private life, 229

Public principles in Software Engineering Code of Ethics, 419–420

Public records, 237, 292–293

Publishing industry, reliability of, 140

Punched card tabulation, 8–9

Purchasing power, 461–462

Python language, 209

Q

Quartering Act, 231

Quotation marks (“ ”) for cited text, 514

Qwest company, 356

R

Race conditions, 371–372

Rachels, James

    on core values, 59

    on ethical egoism, 63

    on social contract theory, 80

Radar systems, 13

Radcliff, Jay, 357

Radiation treatments. *See* Therac-25 linear accelerator

Radio

Internet, 188

invention of, 22–23

Radio frequency ID (RFID) tags, 241–242

Ramirez, Edith, 249

Rand, Ayn, 62

Ransomware, 329–330

Ratings systems, voluntar, 124

Rationalization, 49

Rawls, John

on freedom of expression, 134

principles of justice, 82

social contract agreements, 85

Ray, James Earl, 273

Raza, Ghyslain, 141

RCA Communications, 280

Reagan, Ronald

1984 election, 42
Bork nomination, 299
Real ID Act, 297–298
Real-time systems, 359
Recording Industry Association of America (RIAA)
copyrights, 176
Diamond Multimedia Systems lawsuit, 185
Felten letter, 189
Napster, Grokster, and Kazaa suits, 191–193
Operation Payback attack, 341
Verizon subpoena, 192
Red herring, 528
Reddick, Jaret, 163
Reddick, Shirley, 443
Reddit site
as community, 113
revenge porn, 142–143
Redlining, 392

Reformation, Protestant, 29

Registration, censorship through, 123

Rehnquist, William, 133

Reich, Robert, 480

Reid, Richard, 288

Reiman, Jeffrey

on privacy, 234

on vices, 145

Relativism

cultural, 56–59

subjective, 54–56

Reliability, 353–354

data-entry and data-retrieval errors, 354–356

discussion questions, 401–402

in-class exercises, 402–403

review questions, 400–401

software and billing errors, 356–358

software system failures, 358–367

Therac-25. *See* Therac-25 linear accelerator

Religion in divine command theory, 59–62

Religious Freedom Restoration Act, 303

Remington & Sons Company, 22

Remington Rand Corporation, 11–13

Remote computing, 28

Remote work, 477–479

Reprogramming ENIAC, 9

Republic, The, 101

Research In Motion (RIM), 201

Reshef, Eran, 336

Responsibility

characteristics, 447–448

conditions for, 374

Restaurant reviews, 137

Reuse of code, 374

Revenge porn, 142–143

Reverse engineering, 170–171

Reviews, fake, 137

Rewards programs, 239–240

RFID (radio frequency ID) tags, 241–242

RIAA (Recording Industry Association of America)

copyrights, 176

Diamond Multimedia Systems lawsuit, 185

Felten letter, 189

Napster, Grokster, and Kazaa suits, 191–193

Operation Payback attack, 341

Verizon subpoena, 192

RIAA v. Diamond Multimedia Systems, Inc., 184–185

Rice, Tamir, 341

Rich and poor, growing gap between, 490

Richardson, Elliot, 291

Ridge, Tom, 288

"Right To Privacy, The," 232

Rights

privacy, 231–234

in social contract theory, 82

and software protections, 203–204

RIM (Research In Motion), 201

Rio portable music player, 185

Ripskis, Al, 447

Ritty, James and John, 7

Riven game, 33

Roberts, Lawrence, 25

Robotics, Three Laws of, 458

Roentgen, Wilhelm, 367

Rogan, Terry Dean, 356

Role of social media, 119

Role responsibility, 447

Roosevelt, Franklin, 279, 295

Rootkits, 189, 330

Ross, W. D., 74

Rousseau, Jean-Jacques, 79–80

Roving surveillance, 286

Roving wiretaps, 284

Royal Society for Mental Health, 105

Ruby language, 209

Rule utilitarianism

basis of, 75

case against, 78–79

case for, 77–78

ethical evaluations freedom of expression, 131

ethical evaluations in scenario, 76–77

law breaking in, 95–96

mispriced items, 358

privacy, 236

spam, 110

Russian misinformation campaign, 121

Rutter, Brad, 465, 466

S

Safari browser, 33

Safaricom company, 117

Safe software development, 199–200

Saffo, Paul, 31

Salem, Enrique, 344

Salto, Manuel, 137

Saltzman, Eric, 211

Samsung in smartphone patent wars, 202

Sandwich Islands, 462

Santa Cruz vehicle database, 393

Sarnoff, David, 23

Saturday Evening Gazette, 232

Saudi Arabia, Internet access in, 124

SCADA (Supervisory Control and Data Acquisition), 339

Scanlan, Michael, 165

Scanners

AIT, 303

body, 240–241

Scantlebury, Roger, 25

Scheutz, Georg and Edvard, 6

Schmidt, Eric, 288

Schools, monitoring in, 481

Schor, Juliet, 460, 462

Schumer, Charles, 254

SCMS (Serial Copyright Management System), 184

Scripting, cross-site, 329

Scrolls, papyrus, 29

Scud missiles, 359–360

SDMI (Secure Digital Music Initiative), 188

Search engines, 34

Seatbelts, gender bias in, 437

SEC (Securities and Exchange Commission), 281

Secret Service

cyber attacks on, 338

identity theft investigations, 137

Secrets, trade, 170–171

Secret Web sites, 113

Secure Digital Music Initiative (SDMI), 188–189

Securities and Exchange Commission (SEC), 281

Security, 315–316

cyber crime, 332–342

discussion questions, 344–345

hackings. *See* Hacking

in-class exercises, 345–346

malware, 322–332

monitoring for, 481

review questions, 343–344

worms. *See* Worms

Sega Genesis game console, 198

Sega v. Accolade, 198

Segregation protests, 85

Self-censorship, 123–124

Self-driving cars, 530–532

Self principles in Software Engineering Code of Ethics, 418–426

Semaphore telegraph, 19

sendmail application

    Morris worm, 326

    as open-source software, 210

Sensenbrenner, Jim, 289

September 11 attacks, 281–282

Serial Copyright Management System (SCMS), 184–185

Serious Organised Crime Agency, 341

Service marks, 171

Servicemembers Legal Defense Network, 282

SESAC, 174

Sesame Street channel, 319

Sexting, 134–135

Sexual harassment, 437

S&H Green Stamps, 239

Shakespeare, William, in *Hamlet* scenario, 166–167

Shamrock, Operation, 280–281

Sheep overgrazing problem, 84

Shockley, Bill, 13

Shockley Semiconductor, 13

Shockwave Rider, The, 325

Sholes, Christopher, 22

Shopping, online, 112

Shopping carts, 239, 244

ShopRite stores, 239

Short Pump Town Center mall, 254

Shoulder surfing, 136

Sidejacking, 320–321

Siegel, Martha, 107

Signal Security Agency, 280

Silver Rule, 100

Simons, Bright, 117

"Simple Gifts," 210

Single-computer hypertext systems, 32–33

Sit-ins, 85

Size of passwords, 333

Sjödin, Henrik, 27

Skills development, 415

Skype, NSA access to, 283

Sling video service, 197

Slippery slope argument claims, 526

Small-Scale Experimental Machine, 10

Smart city, 462

Smartphones, 27, 202

Smith, Paul, 132

Snowden, Edward, 113, 283, 389

Social Contract, The, 79

Social contract theory, 79–80

    case against, 85–86

case for, 84–85
ethical evaluations
CIPA, 134
freedom of expression, 130
Internet addiction, 145
spam, 110
sting operation, 139

Social contract theory (*Continued*)
ethical evaluations in
canceled vacation, 463
intellectual property, 179
Internet worm, 328
privacy, 236
scenario, 83–84
law breaking in, 93–94
social contract in, 80–81
theory of justice, 81–83

Social divide, 488

Social engineering, 317

Social equality, 82–83

Social Intelligence Corporation, 238

Social network analysis, 249–250

Social Security Act, 295

Social Security Administration, 295

Social Security numbers (SSNs), 295

Social-technical spam solutions, 108

Socialization, online, 112

Societies

    in cultural relativism, 56–59

    definition, 48

    professional, 416

    winner-take-all, 493–496

Socrates, 53

Software

    and billing errors, 356–358

engineering, 418–426

errors in, 371–372

gender bias, 436–437

open-source. *See* Open-source software

protections for, 197

copyrights, 197–198

legitimacy, 203–206

patents, 200–203

safe development, 199–200

quality of, 425

recommendation scenario, 429–430

software system failures, 358–359

Ariane, 360–361

AT&T long distance network collapse, 361–362

baggage handling systems, 363

Denver International Airport, 363–364

Mars missions, 362

Patriot missile system, 359–360

Tokyo Stock Exchange, 364

voting machine failures, 364–367

system failures, 358–367

Software Engineering Code of Ethics and Professional Practice, 418

alternative fundamental principles, 427–428

analysis of, 426–427

case studies, 428

antiworm, 431–433

child pornography, 430–431

consulting opportunity, 433–435

software recommendation, 429–430

preamble, 418–419, 426–427

principles, 419–426

Software engineers

as professionals, 414–418

Solove, Daniel, 270, 390, 293, 298, 302

Sonny Bono Copyright Term Extension Act, 175–176
Sony
    Betamax lawsuit, 183
    PlayStation 4, 191
    smartphone patent wars, 202
Sony BMG Music Entertainment, 189
Sony v. Universal City Studios, 183–184, 194
Soo, Kim Hyu, 114
Soule, Samuel, 22
Sources
    citing, 514
    misuse, 514
South Korea
    cyber attacks, 338
    gaming in, 114, 147
    Internet addiction, 144, 147
South Ossetia, 337
Southwest Airlines, 353

Soviet Union, censorship in, 123

Space shifting, 185, 213

Space Shuttle disaster, 441–442

Spain, terrorist attack in, 288

Spam

    Blue Frog bot for, 335

    ethical evaluations of, 108–111

    growth, 107

    origin of term, 107

    social-technical solutions, 108

Sparapani, Timothy, 298

Spear, Tony, 362

Spear phishing, 333

Special Subcommittee on Invasion of Privacy, 291

Specialization, 47

Spector Pro program, 132

Speculation, 484

Speelman, Jane, 243

Sperry Rand, 12

Spitzer, Robert, 445

Spock, Benjamin, 281

Spotify music service, 197

Spreadsheet programs, 17

Spyware, 330

    description, 330

    identity theft, 334

SQL injection, 333

SSNs (Social Security numbers), 295

Stacks, HyperCard, 32–33

Stallman, Richard, 205, 207, 209–210

Standard of living, 483

Stanford Research Institute, 31

Star Chamber, Court of, 127

Starbucks, 353

State of nature, 79

Step Reckoner, 6

Stevenson, Adlai, 11

Stewart, Potter, 280

Stibitz, George, 24

Stillwell, Tami, 261

Sting operations, 138–140

Stored Communications Act, 284, 301

Stossier, Sheila Jackson, 354

Stout, Donald, 201

Stratification model, 490

Strip searches, virtual, 303

"Stroke of Geni-Us, A," 187

Sturgeon, William, 18

Stuxnet worm, 339

Subcontractors, 479

Subjective relativism, 54–56

Subscribers in cell phone markets, 250

Subscription music services, 192

Sudafed, 303

Sudduth, Andy, 327

Summer Olympics, 125

Sumner, William Graham, 56

Sun Microsystems, India offices, 482

Sunde, Peter, 196

Sunstein, Cass, 121, 514

Supervisory Control and Data Acquisition (SCADA), 339–340

Supply-chain automation, 477

Supreme Court, United States

- Bork nomination, 299
- *Charles Katz v. United States*, 280
- children Internet access restrictions, 125
- copyrights, 175, 181–182
- *Diamond v. Diehr*, 200
- *FCC v. Pacifica Foundation et al.*, 128–129
- *MGM v. Grokster*, 193–194
- *Nardone v. United States*, 279

Olmstead v. United States, 278–279

smartphone patent wars, 202

Sony v. Universal City Studios, 183, 194

United States v. American Library Association, 132

Weiss v. United States, 279

wiretapping decisions, 283, 284

Surveillance drones, 275

Sweden, privacy laws in, 295

Syllabary writing systems, 28

Syndromic Surveillance System, 294

System/360, IBM, 14

System malfunctions, 356

Systrom, Kevin, 255

T

Tablets, 4–5

Tags

E-ZPass, 300–301

Facebook, 238–239

TALON (Threat and Local Observation Notices) database, 282

Tandy computers, 17

Target

data mining, 247–248

stolen credit cards data, 35

Targeted direct mail, 248–249

Task Force on Heroin Suppression, 281

Taxes

online payments, 114

for winner-take- all effect reduction, 496

Tay, 390

TCL/TK language, 209

TCP (Transmission Control Protocol), 25–26

TCP/IP protocol, 25–26, 33

Technical bias, 390

Technological determinism, 37

Technological diffusion, 489
    models, 489–490
Technological singularity, 472
Telecommunications record database, 294
Telefind Corporation, 201
Telegraph
    harmonic, 21
    invention of, 20
    semaphore, 19
Telemarketing, 302
Telephone records, NSA access, 289–290
Telephone systems, history of, 20–22
Telephony metadata, 289
Teletype machines, 22
Television
    closed-circuit cameras, 275–276
    commercials volume, 302–303
    invention of, 23–24

Telvent Canada, 340

Templeton, Brad, 107

Temporary work, 179

Tenenbaum, Joel, 193

Teresa, Mother, 55

Terms of service, Instagram, 255

Terrorism and Patriot Act, 285–290

Terrorist Screening Database, 295

Tesla Motors (Tesla Version 7.0)

    hand-off problem, 376

    May 2016 Fatal Accident, 375–376

    moral responsibility, 377–378

    SAE Level, 374–375

TeX language, 210

Texas Instruments

    India offices, 482

    integrated circuits developed by, 13–14

Text messaging, 117

Areas with Limited Infrastructure, 117

political activation, 118

sexting, 134–135

Twitter, 117–118

Thampi, Arun, 254

Theory of justice, 81–83

Therac-25 linear accelerator, 367–368

accidents, 368–371

analysis, 372–373

harm from, 417

moral responsibility for, 373–374

postmortem, 372–373

postscript, 374

software errors in, 371–372

Third Amendment, 231

“Thisisyourdigitallife,” 256

Thomas-Rassert, Jammie, 192–193

Thompson, Herbert, 366

Thomson, Judith Jarvis, 232–233

Threat and Local Observation Notices

(TALON) database, 282

Three Laws of Robotics, 458

Thumbnail photographs, 185–186

Tibetan government, cyber attacks on, 338

Tiered services, Internet, 492

Tiger teams, 476–477

Time-sharing, 12–13

Time shifting, 183–184

Time *vs*. possessions, 462–463

Titanic, 23

Title III of the Omnibus Crime Control and Safe Streets Act, 283

Title VII of Civil Rights Act, 437

TiVo, 244

Tokyo Stock Exchange, 364

Tolerance, 55–56

Tollbooth information, 300–301

Tom Sawyer, 22

Tomlinson, Ray, 25

Torah, 59

Torvalds, Linus, 210

Touch screen voting machines, 364–367

Tracking cell phones, 254

Trade secrets, 170–171

Trade unions, 484

Trademarks, 171

Traffic congestion, 113

Tragedy of the commons, 84

Traitorous eight, 13–14

Transistors, 13

Transportation Security Administration (TSA), 303, 305

TransUnion credit reporting agency, 292–293

Trap-and-trace devices, 283–284

Treasury Department, cyber attacks on, 338

Trojan horses, 329

    from rootkits, 189

Trolley problem, 476

Trump, Donald, 119, 256, 387

Truncation errors, 359

Trust and privacy, 234–235

TSA (Transportation Security Administration), 303, 305

Tsinghua University, 486

Tunisia, 118, 341

Turner, Clark, 372

Twain, Mark, 22

Tweets, 117–118

Twitter

    HTTPS option, 321

    revenge porn, 142–143

“Twitter Dashboard,” 118

Two-factor authentication, 317

Typewriters, 22

U

Uber company, 479–480

Uber test-vehicle accident, 378–380

Uconnect software, 357

Udall, Mark, 289–290

Ukraine, cyber attacks against, 341–342

Unemployment from automation, 458–464

Unfair debating gambits, 528–529

Uniform Resource Locators (URLs), 112

United Kingdom

    privacy report, 291

    revenge porn, 142–143

United States, cyber attacks in, 338

United States v. American Library Association, 132

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), 285

National Security Letters, 286–287

NSA access to phone records, 289–290

provisions, 285–286

responses, 287–288

successes and failures, 288–289

UNIVAC computer, 10–12

Universal City Studios, 183–184, 194

Universal law in Categorical Imperative, 66–67

Universities

contingent faculty members, 479

online, 113

University of Kansas, 318

University of Manchester, 10

University of Nevada, 318

University of Virginia, 513

Unix operating system

GNU project, 209

security holes in, 325–326

Unsafe working conditions, 36

Unsound arguments, 523–524

Uploads, address book, 254–255

URLs (Uniform Resource Locators), 112

USA Freedom Act, 290

USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and 0 bstruct Terrorism Act), 285

National Security Letters, 286–287

NSA access to phone records, 289–290

provisions, 285–286

responses, 287–288

successes and failures, 288–289

Utilitarianism

act, 70–75

ethical evaluations in
canceled vacation, 463–464
CIPA, 133–134
Firesheep case, 320–322
freedom of expression, 131
intellectual property, 179–180
Internet addiction, 145
Internet worm, 328
spam, 109
sting operation, 138–139
NCIC records, 355–356
privacy, 236
rule, 75–79
on software protection, 204–206
Utility, Principle of, 70–71, 75

V

Vacations, 463–465

Vacuum tubes for signal amplifiers, 13–14

Vaidhyanathan, Siva, 175

Validation

arguments

affirming the antecedent, 520–521

chain rule, 522

denying the consequent, 521

process of elimination, 521–522

VCR sales, 489

Vellum, 29

Verichip Corporation, 242

Verizon, 192

Vices, 88

Video Privacy Protection Act, 299

Video recorders, digital, 244

Video streaming services, 197

Vietnam war

counterculture from, 15

watch lists during, 281–282

Virginia Declaration of Rights, 127

Virginia Information Technology Agency (VITA), 366–367

Virtual strip searches, 303

Virtual worlds, 114

Virtue ethics, 86–92

case against, 91–92

case for, 90–91

ethical evaluations in

Firesheep case, 321–322

intellectual property, 180–181

Internet worm, 328

spam, 110

scenario for, 89–90

Viruses, 323–325

minimizing, 378

spread of, 323–325

Visa, Operation Payback attack, 341

Visas, work, 485–486

VisiCalc program, 17

VisiCorp Corporation, 32

Voice of America, 125

Voice over Internet Protocol (VoIP), 285

Volta, Alessandro, 18

Voluntary information disclosures, 238–239

Vonnegut, Kurt, Jr., 458

Voter News Service, 24

Voters, disenfranchised, 354

Voting machines, 364–367, 398

W

Wages

CEOs vs. production worker, 494–495

and low unemployment, 458

Wake County voting machine errors, 366

Walt Disney Corporation, 176

Walt Disney Productions, 183

War in Iraq

looting in, 79

self-censorship in, 123–124

War of the Worlds, 23

Warg, Gottfrid Svartholm, 195–196

WarGames, 315

Warner Music Group, 169–170

Warren, Samuel, 231–232

Warschauer, Mark, 498

Watch lists for crime figures, 280–281

Watson, Thomas A., 21

Watson, Thomas J., 9

Watson program, 465–466

Waze app, 113

WBAI radio station, 129

Wealth

digital divide, 487–493

discussion questions, 500–502

dot-com bust, 484–485, 498

in-class exercises, 502–503

review questions, 499–500

winner-take-all society, 493–497

Web. *See* World Wide Web (WWW)

Web 2.0, 113

Web-accessible pharmacies, 459

Weinstein, Lauren, 297, 438

Weiss v. United States, 279

Welles, Orson, 23

Western Union, 280

Whistle-blowing, 440

Hughes Aircraft case, 442–444

legislation, 444

morality of, 445–448

Morton Thiokol case, 441–442

and organizational failure, 445–446

Whistleblower Protection Act, 444

White, Nicholas, 137

White-collar jobs lost, 459–460

White-Smith Music Company, 175–176

Whole Earth Catalog, 15–16

Wi-Fi networks, 322

Wiggins, Calvin, 442

WikiLeaks, 333, 341

Wikipedia, 113

Wikis, 113

Williams, F. C., 10

Williams, Samuel, 24

Williams Tube, 10

Windows Media Player, 189

Windows systems, 31

Winner-take-all society

development of, 495–496

harmful effects, 495–496

reducing harm from, 495

Winner-Take-All Society, The, 498

WinVote DRE system, 366–367

Wire Fraud Act, 318

Wireless networks, 27, 481

Wiretapping

history, 278–280

legislation authorizing, 282–285

NSA, 281–282

roving, 283–284

Wolpe, Howard, 359

Women

data mining targeting, 247–248

gender bias, 436–437

Wood engraving, 29

Woolworth's store, 85

Working conditions, 36

Workplace. *See* Jobs

monitoring, 481

multinational teams, 482

organization changes in, 476–477

temporary work, 479

World of Warcraft game, 149

World Trade Center, 285

World Trade Organization (WTO), 483

World Wide Web (WWW)

attributes, 111–112

children on, 131–135

development of, 33

false information, 140

filters for, 132

open-source servers, 208–209

search engines, 34

WorldWar I, 272

WorldWar II
computing device development, 9–10
personal data collection, 413
wiretapping, 279, 280
Worms
antiworm scenario, 431
Internet, 325–329
types, 325–329
Wozniak, Steve, 16–17
Writing Program Administrators (WPA), 513
Writing *systems*, 28–29
Writs of assistance, 278
WTO (World Trade Organization), 483
WWW (World Wide Web)
attributes, 111–112
children on, 131–135
development of, 33
false information, 140

filters for, 132

open-source servers, 208–209

search engines, 34

Wyden, Ron, 289

X

X-rays. *See* Therac-25 linear accelerator

X Window System, 210

Xanadu network, 30

Xbox One, 190–191

Xerox Corporation, 31, 172

Xiamoni in smartphone patent wars, 202

Y

Yahoo

government request for email, 283

tiered services opposition, 492

Yahoo!Mail, Blue Frog bot for, 335

Yakima Valley Memorial Hospital, 369, 371–372

Yard, Margaret, 460

Yelp restaurant reviews, 137

Young, Kimberly, 145

Z

Zeus Trojan Horse, 336

Zillow.com site, 227, 237

Zombie computers, 108

Zones of inaccessibility, 228

Zoning laws, 128

Zope language, 209

Zuckerberg, Mark, 254, 257

Ninth Edition

MICHAEL J. QUINN

ETHICS

FOR THE INFORMATION AGE

Ethics for the Information Age

9th edition

MICHAEL J. QUINN

Seattle University

221 River Street, Hoboken, NJ 07030

Content Management: Tracy Johnson
Content Production: Dr. Rajul Jain, Rajinder Singh
Product Management: Tracy Johnson
Product Marketing: Krista Clark
Rights and Permissions: Rogini Rajendiran, Chandan Kumar, Vignesh Murugamoorthy

Please contact www.AskPearsonSupport.com with any queries on this content.

Pearson puts care into the creation of our products. Our learning materials undergo content reviews to minimize bias and ensure the content is inclusive, accurate, and relevant. Please use this link to report instances of bias and inaccuracies: https://www.pearson.com/report-bias.html

You can learn more about Pearson's commitment to accessibility at https://www.pearson.com/us/accessibility.html

Cover Image by: Metamorworks/Shutterstock

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any

kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Copyright © 2025, 2020, 2017 by Pearson Education, Inc. or its affiliates, 221 River Street, Hoboken, NJ 07030. All Rights Reserved. Manufactured in the United States of America. This publication is protected by copyright, and permission should be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise. For information regarding permissions, request forms and the appropriate contacts within the Pearson Education Global Rights & Permissions department, please visit https://www.pearson.com/global-permission-granting.html.

Acknowledgments of third-party content appear on the appropriate page within the text.

PEARSON is exclusive trademark owned by Pearson Education, Inc. or its affiliates in the U.S. and/or other countries.

Unless otherwise indicated herein, any third-party trademarks that may appear in this work are the property of their respective owners and any references to third-party trademarks, logos or other trade dress are for demonstrative or descriptive purposes only. Such references are not intended

to imply any sponsorship, endorsement, authorization, or promotion of Pearson's products by the owners of such marks, or any relationship between the owner and Pearson Education, Inc. or its affiliates, authors, licensees or distributors.

Library of Congress Cataloging-in-Publication Data

Names: Quinn, Michael J. (Michael Jay), author.

Title: Ethics for the Information Age / Michael J. Quinn, Seattle University.

Description: Ninth edition. | Hoboken, NJ : Pearson, [2025] | Includes bibliographical references and index.

Identifiers: LCCN 2023057085 | ISBN 9780138238537 (hardcover)

Subjects: LCSH: Electronic data processing—Moral and ethical aspects. | Information technology—Moral and ethical aspects. | Computer networks—Moral and ethical aspects. | Computers and civilization.

Classification: LCC QA76.9.M65 Q56 2024 | DDC 004—dc23/eng/20240109

LC record available at https://lccn.loc.gov/2023057085

$PrintCode

ISBN-10: 0138238758

ISBN-13: 9780138238759

Brief Contents

Preface

1 Catalysts for Change

2 Introduction to Ethics

3 Networked Communications

4 Intellectual Property

5 Information Privacy

6 Privacy and the Government

7 Computer and Network Security

8 Computer Reliability

9 Professional Ethics

10 Automation and Globalization

Appendix A: Plagiarism

Appendix B: Introduction to Argumentation

Index